RAND EUROPE

CHILDREN AND FAMILIES
EDUCATION AND THE ARTS
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INFRASTRUCTURE AND TRANSPORTATION
INTERNATIONAL AFFAIRS
LAW AND BUSINESS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
TERRORISM AND HOMELAND SECURITY

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis.

This electronic document was made available from www.rand.org as a public service of the RAND Corporation.

Skip all front matter: Jump to Page 1

Support RAND

Browse Reports & Bookstore

Make a charitable contribution

For More Information

Visit RAND at www.rand.org

Explore RAND Europe

View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND electronic documents to a non-RAND Web site is prohibited. RAND electronic documents are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see RAND Permissions.

This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

Information Security and Data Protection Legal and Policy Frameworks Applicable to European Union Institutions and Agencies

Neil Robinson, Jan Gaspers

RAND EUROPE

EUROPE

Information Security and Data Protection Legal and Policy Frameworks Applicable to European Union Institutions and Agencies

Neil Robinson, Jan Gaspers

Sponsored by Microsoft Europe

The research described in this report was sponsored by Microsoft Europe.

RAND Europe is an independent, not-for-profit policy research organisation that aims to improve policy and decisionmaking for the public interest though research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark

© Copyright 2014 RAND Corporation

Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Copies may not be duplicated for commercial purposes. Unauthorized posting of RAND documents to a non-RAND website is prohibited. RAND documents are protected under copyright law. For information on reprint and linking permissions, please visit the RAND permissions page (www.rand.org/publications/permissions.html).

RAND OFFICES

SANTA MONICA, CA • WASHINGTON, DC

PITTSBURGH, PA • NEW ORLEANS, LA • JACKSON, MS • BOSTON, MA

DOHA, QA • CAMBRIDGE, UK • BRUSSELS, BE

www.rand.org • www.rand.org/randeurope

Preface

This Research Report reviews the legal and policy frameworks that govern the use of information and communications technology by European Union institutions and agencies in terms of the extent to which they account for information security and data privacy. The Report thus informs evolving debates about the complex range of information security and data protection obligations to which the EU institutions and agencies are increasingly subject.

The authors would like to thank the reviewers Dr Matt Bassford (RAND Europe) and Hans Graux (time.lex) for their useful feedback and constructive support with regard to prepare this Research Report. The authors would also like to thank Alex Hull for his support in preparing this document for publication.

Last but not least, we gratefully acknowledged the financial support we received from Microsoft Europe to conduct the study presented in this document.

RAND Europe is an independent not-for-profit policy research organisation that aims to improve policy and decision making in the public interest, through research and analysis. RAND Europe's clients include European governments, institutions, NGOs and firms with a need for rigorous, independent, multidisciplinary analysis.

For more information about RAND Europe or this Research Report, please contact:

Neil Robinson
Research Leader

RAND Europe
Rue de la Loi, 82
Brussels B-1080
Belgium
+32 (0)2 6692401
Neil_Robinson@rand.org

Table of Contents

Summary

This study examines the legal and policy frameworks that govern and regulate the use of information and communications technology (ICT) by European Union (EU) institutions and agencies. Specifically, it maps and reviews these frameworks in terms of the extent to which they account for information security and data privacy.

The study pursues a two-fold research approach. First, it offers a largely descriptive account of the existing legal and policy frameworks that govern and regulate the use of ICT by EU institutions and agencies, summarising in particular those legal provisions and policy documents that address information security and data privacy issues.

Second, the study offers some general observations based on the summary of legal and policy frameworks that regulate and govern the use of ICT by EU institutions and agencies. Significantly, these observations are neither intended to amount to a comprehensive analysis of existing EU legal and policy instruments on information security and data privacy, nor are they meant to provide any recommendations for EU policy-making. Instead, they aim to build a general understanding of the way in which relevant EU legal and policy frameworks might affect the adoption of new technologies by EU institutions and agencies. More fundamentally, it is hoped that by mapping and summarising, in an accessible format, the canon of relevant EU legal and policy frameworks, this study will create a greater awareness of the conditions under which ICT is used within EU institutions and agencies.

The first set of findings is presented in Chapter 2, which shows that the specific ICT usage requirements of different EU institutions and agencies also impose specific information security and data privacy requirements on ICT infrastructure. These ICT usage requirements relate to a wide range of different policy domains, including:

- Support to information exchange and cooperation between Member States on EU internal policies with external components (such as the internal market, customs, etc.).
- Big data challenges relating to the collection and processing of geospatial imagery data.
- The processing of police and criminal justice data.
- The protection of classified information in multinational environments.

While vital EU ICT infrastructure (such as sTESTA, OPSWAN and SIS II) has specific in-built resilience frameworks, it often lacks in security incident notification mechanisms.

More generally, Chapter 2 finds that legacy equipment, path dependency when it comes to law and policymaking, and the natural conservativeness of a large and complex administrative machine may act as inhibitors to building greater information security in EU institutions and agencies.

Examining legal and policy frameworks that govern and regulate the use of ICT across EU institutions and agencies, Chapter 3 finds that:

- The overall tone of EU policy and legal frameworks governing and regulating information security resonates with a model of security based on an internally secure organisation and insecure external environment, which appears to be inconsistent with the latest evolving canon of best practice concerning inter-organisational security, as, for example, codified by the International Standards Organisation.
- Key EU information security and data protection frameworks would appear poorly aligned with many modern models of technology service delivery and use, including cloud computing, the consumerisation of IT ('bring your own device'), service-orientated architectures (SoA), and an open model of IT services mediated through cyberspace. For example, although the e-Commission Communication flags up the involvement of the European Commission in the Cloud Computing Strategy, it is not clear that existing security frameworks are also aligned.
- The potential for security and privacy requirements to be built in from the start through Security Engineering or Privacy by Design principles appears to have little visibility in many of the EU legal and policy frameworks this study covers.

Mapping legal and policy frameworks, which cover policy domains that are unique to EU institutions and agencies, such as the management and processing of sector-specific data, the processing of personally identifiable nominal data for intelligence, border management and criminal justice cooperation, or the processing of sensitive classified information for EU-led crisis management operations, Chapter 4 reveals that:

- There is a complex landscape of very specific information security and data protection requirements for different EU policy domains.
- The unique nature of some of these policy domains and their attendant security or privacy considerations seem difficult to reconcile with the appetite for more innovative types of technology provision (e.g. through greater consumerisation of corporate IT assets or greater use of cloud computing).
- Understanding information security governance and data protection remains a challenge within many EU frameworks, which are often managed in a federated fashion through obligatory standards and rules set at a strategic EU level (either through the EU Council or Council of Europe) and implementation at the national level.

1. Introduction

This study examines the legal and policy frameworks that govern and regulate the use of information and communications technology (ICT) by European Union (EU) institutions and agencies. Specifically, it maps and reviews these frameworks in terms of the extent to which they account for information security and data privacy.

1.1 Research approach

This study pursues a two-fold research approach. First, it offers a largely descriptive account of the existing legal and policy frameworks that govern and regulate the use of ICT by EU institutions and agencies, summarising in particular those legal provisions and policy documents that address information security and data privacy issues. In this context, the study also touches upon the way in which some of these frameworks might affect public and private stakeholders within EU Member States, third states and international organisations.

As is shown in subsequent chapters, there are substantial numbers of legal and policy instruments already in place with regard to the use of ICT in various EU policymaking spheres and domains. The latter encompass:

- Horizontal frameworks dealing with data protection, information security, document management and the protection of classified information (in a range of business activities, such as human resources, pensions, e-procurement and business continuity).
- The internal market (e.g. European Carbon Trading Emissions or the exchange of VAT data).
- The Area of Freedom, Security and Justice (AFSJ), covering the activities and systems of the EU supporting cooperation between Member State criminal justice systems, including large-scale IT systems in the areas of justice and home affairs and e-justice.
- The Common Security and Defence Policy (CSDP) and the Common Foreign and Security Policy (CFSP), covering the activities of EU institutions and agencies with regard to CSDP crisis management operations and the conduct of foreign policy.

Secondly, the study also offers some general observations based on the summary of legal and policy frameworks that regulate and govern the use of ICT by EU institutions and agencies. Significantly, these observations are neither intended to amount to a comprehensive analysis of existing EU legal and policy instruments on information security and data privacy, nor are they meant to provide any recommendations for EU policymaking. Instead, they aim to build a general understanding of the way in which the relevant EU legal and policy frameworks currently in place or under review might affect the adoption of new technologies by EU institutions and agencies. More fundamentally, it is hoped that by mapping and summarising, in an accessible format, the canon of relevant EU legal and policy frameworks, this study will create a greater awareness of the conditions under which ICT is used within EU institutions and agencies.

In discussing the relationship between existing EU legal and policy instruments on information security and data privacy and the adoption of new technologies, the study touches upon a wide range of technological developments and the questions they might raise, including:

- Building resilience into IT: do IT solutions have the resilience to cope with the modern threat environment? Do the existing legal and policy frameworks in EU institutions and agencies relating to security and privacy satisfactorily address the latest thinking on resilience and security in cyberspace?
- Flexible work style, i.e. 'bring your own device' (BYOD)[1] and mobile world: how do the trend for consumerisation and the use of personal devices for work (and vice versa) affect security and privacy and how does the ongoing push for ever greater remote access to core enterprise applications impact upon security and privacy policies and guidance? Are existing legal and policy frameworks in EU institutions and agencies relating to security and privacy viable given the increasing consumerisation of IT?
- Cloud computing adoption: as cloud computing becomes an increasingly popular option, what specific security and data protection issues need to be considered before moving wholesale into the cloud? Do existing legal and policy frameworks in EU institutions and agencies relating to security and privacy prohibit or enable cloud computing adoption?

This research also builds upon a previously developed mapping of the inter-relationships of relevant EU institutions and agencies regarding cybersecurity policy more generally, which was first presented in a study prepared in mid-2013 for the European Parliament (Robinson et al. 2013).

[1] 'BYOD' is a term that reflects the increasing popularity of employees using their own technology (smartphones, tablets or personal computers) in a work environment.

1.2 Methodology

This study is first and foremost based on desk research. We collected known examples of legal and policy frameworks, rules and guidance, then analysed and summarised them. The collection process involved structured searches of online information. We also investigated footnotes and literature pertaining to each relevant institution, conducting reviews of institution websites and annual reports. To fill remaining blanks and to gain a better understanding of EU legislation not publicly available, we also informally consulted with a subject-matter expert.

1.3 The European Union institutions and agencies

In this report we use the term EU institutions and agencies to refer to the following bodies (which make for a non-exhaustive list):

- The European Commission
- The European Parliament
- The Council of the EU
- The European External Action Service (EEAS)
- The Executive Agencies (for example the Research Executive Agency or the Trans European Network Executive Agency)
- Specialised agencies and decentralised bodies (for example, the European Network and Information Security Agency (ENISA), the European Police Office (Europol), the Computer Emergency Response Team for the European Institutions (CERT-EU), and the European Data Protection Supervisor (EDPS)).

2. European Union ICT requirements and infrastructure

This chapter shows that the specific ICT usage requirements of different EU institutions and agencies also impose specific information security and data privacy requirements on ICT infrastructure. These ICT usage requirements relate to a wide range of different policy domains, including:

- Support to information exchange and cooperation between Member States on EU internal policies with external components (such as the internal market, customs, etc.).
- Big data challenges relating to the collection and processing of geospatial imagery data.
- The processing of police and criminal justice data.
- The protection of classified information in multinational environments.

While vital EU ICT infrastructure (such as sTESTA, OPSWAN and SIS II – see below) has specific in-built resilience frameworks, it often lacks in security incident notification mechanisms. More generally, we find in this chapter that legacy equipment, path dependency when it comes to law and policymaking, and the natural conservativeness of a large and complex administrative machine may act as inhibitors to building greater information security in EU institutions and agencies.

2.1 ICT use by EU institutions and agencies

Before summarising in detail EU cybersecurity legal and policy frameworks addressing pertinent security and privacy issues, we discuss here some aspects of the rationale for the usage of ICT by EU institutions and agencies, summarising the business and operational context for the use and dependence of these institutions and agencies upon ICT.

The EU institutions and agencies collectively are, with the exception of the United Nations (UN), perhaps the most prominent and institutionally sophisticated supranational entity in the world. Understanding the use these bodies make of ICT and cyberspace is therefore invariably complex. Like any large public sector organisation, EU institutions and agencies pursue several key administrative functions, like the recruitment and management of employees, the management of sensitive information, furnishing access to official

documents to meet transparency goals, or the management of financial, procurement and invoicing data from suppliers. In other contexts, EU institutions and agencies have more specific IT operational requirements, which raise certain challenges. These stem, in particular, from the scale and cross-border nature of pan-EU initiatives. Examples include the storage and sharing of certain types of nominal (personal) data about suspects and victims in Europol's intelligence databases, types of identifying data about individuals, objects in pan-European databases, such as the second-generation Schengen Information System (SIS II), data about border documents, and the protection of highly classified documents in the context of EU-led CSDP Operations or foreign and security policy.

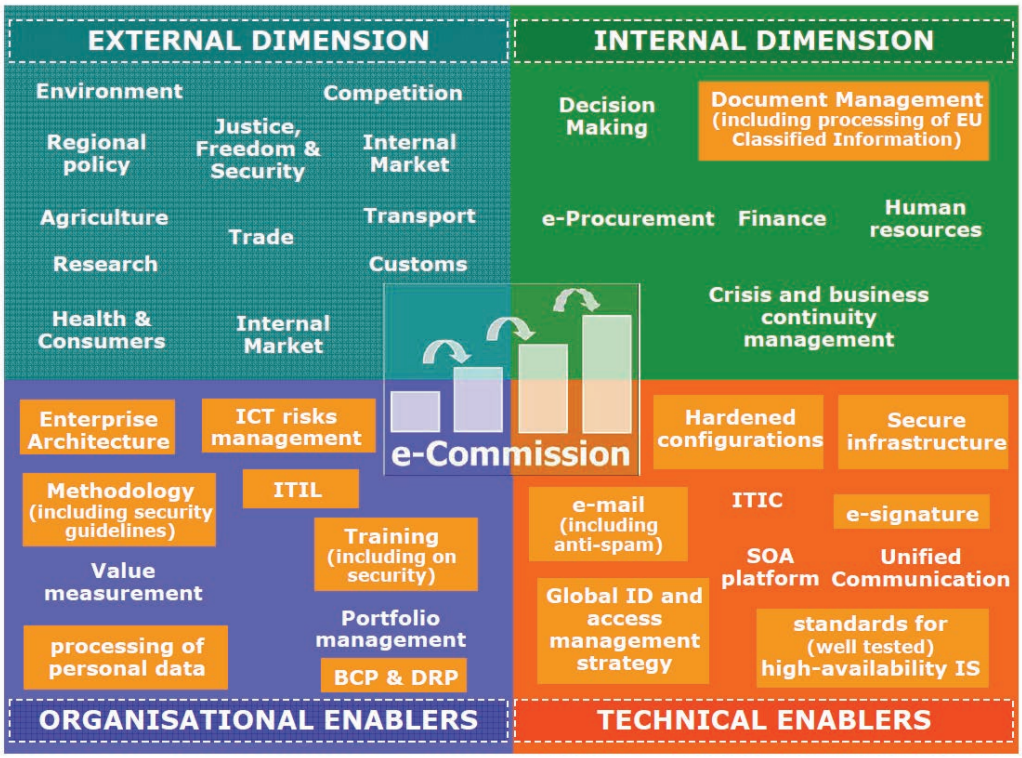
2.2 The e-Commission Initiative 2012–2015

The e-Commission Initiative 2012–2015 follows on from the e-Commission Initiative 2006–2010 (which set out how the European Commission aimed to implement objectives identified in the e-Government Action Plan), the 2009 Digital Agenda, and rationalisation exercises begun in 2010 under Commission Vice President (VP) Šefčovič (European Commission 2010, 2011).

The e-Commission Initiative 2012–2015 sets out a number of actions according to principles under a common vision of 'delivering efficiently, effectively and transparently user-centric digital services and IT solutions to support both EU policies and the Commission's own internal administration' (European Commission 2012a: 5).

The internal- and external-facing dimension of how ICT supports these aims was also reflected in a 2012 presentation by the Directorate-General for Informatics (DIGIT). This presentation characterised the internal and external dimensions of ICT usage, covering policy areas such as the environment, trade and transport, and internal business processes such as e-procurement, decision making, finance and document management (see Figure 2.1).

Figure 2.1: The drivers of ICT usage



Source: Moran (2010)

2.2.1 Security and privacy in the e-Commission Initiative 2012–2015

In the 2012 e-Commission 2012–2015 Communication a specific section on privacy and security was included, which specifies that each Commission initiative must 'guarantee the privacy of citizens and the confidentiality of information provided by businesses' (European Commission 2012a: 7). It noted that its future vision would be further developed by 'improving trust by enhancing IT security' (European Commission 2012a: 6).

This Communication clearly identified security and privacy as organisational enablers, noting that progress had been made since 2010 on a number of actions in the area of security, including:

- Enhancing resilience and failover facilities for the Data Centre and telecommunications network.
- Managing the sTESTA Network that connects Member States public administrations.
- Deploying strong user authentication through ECAS.

The Communication further indicated that the specific needs of each European public service would be considered within the context of a common security and privacy policy.

Specific actions outlined in the Communication relating to security included:

- Protection of the corporate infrastructure (extension of access and identity management system).
- Implementation of an IT security policy framework.
- Reinforcing business continuity management of the Commission's critical services and systems.
- A corporate user authentication system as the mandatory building block for all Commission information systems.

2.3 Cross-cutting activities of EU institutions and agencies

As mentioned above, the EU undertakes a range of cross-cutting activities, which are relatively common across public administrations, such as procurement, invoicing, human resources and personnel, finance, audit and access to public documents. The list below gives examples of some of the IT systems the European Commission, which is by far the largest of the EU institutions, uses to perform such activities:

- ABAC: Financial and accounting system.
- ASSMAL 2: Tools for the sickness and accident insurance scheme.
- e-Prior (electronic procurement, invoicing and ordering): An end-to-end procurement solution for the Commission, including pre-awarding (European Commission 2012b).
- e-Greffe: A system used to support the unique decisionmaking processes of the Commission.
- HERMES-ARES : A corporate document management lifecycle solution (registration, filing, conservation and transfer to archives).
- MyIntraComm: A corporate Intranet and collaboration tool.
- SYSPER2: Tools for human resources and management of employees.

In relation to the IT infrastructure that the European Commission uses to perform these and other relevant activities not listed above, the 2012 e-Commission Communication references the ITIC (IT Infrastructure Consolidation plan) and, based on the European Cloud Strategy, plans to get involved in the active adoption of cloud computing through participation in a series of cloud computing pilots to be launched between 2012 and 2015 (European Commission 2012c).

Finally, other initiatives to exploit innovative technologies such as service-orientated architectures (SoA), mobile computing and telecommunications are also covered in the Communication, but with notably little detail being provided aside from the initiative regarding the upgrade to sTESTA (see below).

2.4 The EU as a provider of infrastructure to Member States

A second set of relevant IT building blocks are at the heart of activities performed by EU institutions and agencies in their role as a provider of underlying IT systems, without necessarily being the end-users of the data. These systems are normally run over the EU wide secured data network known as the secured Trans European Services for Telematics between Administrations (sTESTA). It is thought that there are over 90 different applications that use sTESTA (Wellens 2013). Below we list some indicative examples of sTESTA-based applications or services that facilitate interaction between Member States (as well as EU institutions and agencies) within the framework of common EU activities:

- Carbon / Emission Trading Systems (ETS): The purchase, issuance and trading of carbon emissions permits and the standardised and secure system of registries.
- Digital tachygraphy: The exchange of recorded tachograph information between road haulage companies across the EU to ensure that drivers and companies meet EU requirements regarding safety (e.g. rest stops).
- ECAS: The European Commission's Authentication Service, which provides authentication services for a range of Commission services.
- E-Justice Portal: The exchange of legal information including court rulings and possibly small claims via the e-Justice Portal.
- Eurocontrol: The exchange of air traffic control data by Airspace Management Authorities in the EU in order to improve harmonisation and facilitate efficiency in controlled airspace above Europe.
- Internal Market Information System (IMI): Communication between national, local and regional authorities.
- Participants portal for Research Grants through the Horizon 2020/FP7 programme.
- Services: Reconciliation of payments under the Payment Services Directive.
- SFC2007 System: Management of shared funds between the Member States and the European Commission (DG REGIO, DG EMPL, DG AGRI and DG MARE).
- Single European Payment Area (SEPA) Direct Debits: Coordinating activities aimed at the speedy and accurate reconciliation of direct debits between bank accounts across the EU in conjunction with the European Payments Council.
- VAT Regulations: The exchange of VAT data between Member States to normalise the internal market with regard to transactions incurring VAT.

2.4.1 Secured Trans European Services for Telematics between Administrations (sTESTA)

As the preceding examples illustrate, sTESTA is a European backbone network that facilitates and supports the implementation of EU policy by enabling data exchange among

and between EU Member States and EU institutions and agencies. In fact, sTESTA may be thought of as a network of networks, which links a EuroDomain backbone to local domain networks, including national and regional networks, as well as EU Institution and Agency networks. sTESTA's domain-based approach allows national and regional administrations to connect to European information sources without sacrificing network implementation autonomy. While decentralised in terms of infrastructure, sTESTA's operation is centrally managed under the auspices of DIGIT. The central management is also responsible for the provision of information on the use and integration of sTESTA services within national and regional administrative networks.

Since sTESTA caters for the exchange of both unclassified and classified information, several security measures have been implemented. Thus, despite using the Internet Protocol (IP) to ensure universal reach, the EuroDomain backbone network is operated independently from the public Internet, limiting access rights to administrators. Data security is further enhanced by the application of Internet Protocol Security (IPsec) technology and other advanced encryption mechanisms. Moreover, to ensure Information Assurance, sTESTA's vital components are duplicated and its entire infrastructure is proactively monitored.

Recent years have seen a steady increase in the use of sTESTA, with total network traffic volume having grown rapidly. Indeed, in addition to EU Member States and EU institutions and agencies, a growing number of specialised EU entities have been using sTESTA's services for sectoral applications (e.g. OLAF, DG MOVE DG ESTAT, DG JUSTICE DG SANCO, CDT, DG MARE DG ENV, and DG TRADE). As one of the most recent additions to the group of sTESTA community members, the General Secretariat of the Council has used the sTESTA framework for the implementation of the FADO network, the Council Extranet and the Courtesy network (see below).

With plans for the linkage of EU candidate and European Free Trade Agreement (EFTA) countries to sTESTA maturing, sTESTA traffic is expected to further increase in the future. To meet the additional demand for sTESTA services and the individual needs of the different sTESTA communities and to ensure sTESTA's continued resilience, the EuroDomain backbone network is currently being upgraded. Under a framework contract of a maximum duration of seven years awarded by the European Commission in 2013, Deutsche Telekom's IT subsidiary T-Systems is expected to deliver the 'sTESTA Next Generation (NG)' network, which will feature data transfer rates of up to one gigabit per second as well as the latest security and encryption technology.

Significantly, in recent years EU Member States have not only used sTESTA to implement EU policy but also to realise projects outside the EU framework, such as trans-border police cooperation in the context of the Prüm Treaty or the Financial Intelligence Unit network, which tackles international money laundering and the financing of terrorism (see below).

2.5 Activities unique to EU institutions and agencies

There are three high-level areas where activities performed by EU institutions and agencies are especially unique:

- Pan-European activities related to civilian domains such as monitoring from space and space exploration, and management of the single European Market.
- Measures providing an Area of Freedom Security and Justice (AFSJ), including the collection and sharing of criminal justice information (through Europol and Eurojust); processing of information on border security and management (Frontex) and other information management conducted for the purposes of border security (SIS II, VIS, EURODAC and BMS).
- Common Foreign and Security Policy (CFSP) including the 24 operations of the EU under the Common Security and Defence Policy (CSDP), ranging from humanitarian assistance to armed combat to separate warring parties and EU foreign policy, e.g. connection with EU missions overseas in third countries (Rehrl & Weisserth, 2012).

2.5.1 European Space Agency

The European Space Agency (ESA) delivers a number of services related to the coordination of Member State space activities, and direct and indirect operational control of unmanned space programmes. The most prominent programmes benefitting from the provision of such services are the Copernicus Earth Observation Programme and the SuperSites Exploitation Platform.

Copernicus Earth Observation Programme

Launched in 1998 and previously known as the Global Monitoring for Environment and Security (GMES) programme, Copernicus is an Earth observation programme that collects information in order to improve the management of the environment and understand and mitigate the effects of climate change. Copernicus is currently run under the auspices of the European Commission in partnership with ESA and the European Environment Agency. The space component of Copernicus, which is managed by ESA, will become operational after the launch of the first Sentinel mission in 2014. The 'on the ground' component is managed by the EEA and focuses on generating data from a multitude of sensors on the ground, at sea and in the air.

Copernicus provides a unified system through which vast amounts of data, acquired from space and from a multitude of on-the-ground sensors, are fed into a range of thematic information services that cover six main categories, namely land management, the marine environment, the atmosphere, emergency response, security and climate change.

While each ground segment is independent, they are all linked to form the Copernicus Ground Segment. The Data Access Coordinated System is managed directly by ESA, while other parts are managed by third parties such as National Space Agencies, and interface to the core ESA elements via specific agreements with the Agency.

The overall space capacity, beyond the single missions, is coordinated through the Copernicus Space Component Data Access System. This is carried out in agreement with contributing data providers. The system provides comprehensive and coordinated access to space data, to:

- Link transparently the different data providers and the various Copernicus services using specific coordinating functions.
- Create synergy and sustainability across the various contributing missions.
- Access a simplified interface for advertisements and the service desk rather than using multiple data provider interfaces.

The system is the hub of an interoperable network of distributed European ground segments contributing to Copernicus, culminating in a harmonised, one stop shop for users.

Data and services are accessible in the form of datasets, which are pre-defined collections of coherent (single and/or multi-mission) products that are derived from service requirements after trade-off considering the overall capacity of the space component.

SuperSites Exploitation Platform

In September 2013, ESA launched the SuperSites Exploitation Platform (SSEP), which is a geohazards research platform through which researchers worldwide can analyse large amounts of satellite earthquake and volcanic data. One of SSEP's main purposes is to complement legacy systems, which are based on the physical transfer of data among participating research institutions and the processing of data on researchers' premises.

SSEP takes the form of a private cloud service-based Virtual Data Centre, through which participating scientists have permanent access to 13 terabytes of geohazards data. Specifically, scientists can draw on cloud-based scalable on-demand processing, collaboration tools, and a range of algorithms to process and share information with virtual research communities around the planet. Moreover, SSEP's cloud toolbox offers virtual desktop resources, configured with software and licences for analysing and processing the data.

2.5.2 Europol

Europol is the EU's criminal intelligence agency. It is not an operational body as such but has a mandate to support cooperation between EU Member States. It hosts intelligence databases (driven by contributions from Member States), runs analysis, provides support (e.g. in the form of the European Computer Forensic Network), and also helps with training and education activities for law enforcement and judicial personnel.

Europol Information System (EIS)[2]

One of Europol's core databases is the Europol Information System (EIS), through which EU Member States can share and retrieve information about persons, events and items related to a criminal case (e.g. suspects, weapons, phone numbers, number plates, or passports).

[2] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol).

The range of data that may be processed in the EIS is limited in a number of ways that are necessary for achieving Europol's criminal intelligence tasks (see Chapter 4). Such data includes nominal information (e.g. various types of personal data) and must relate to suspects and persons of interest to the criminal intelligence community.

In recent years, specifically designed dataloaders have been installed in many national databases to automatically upload relevant data to Europol. Organisational and technological safeguards are in place to ensure that only data that comply with Europol's mandate are transmitted, creating an element of 'privacy by design'.

Secure Information Exchange Network Application (SIENA)

In addition to the EIS, a tailor-made messaging system has been implemented at Europol. The Secure Information Exchange Network Application (SIENA) facilitates the swift exchange of information among EU Member States. The SIENA infrastructure is hosted in Europol's New Headquarters.

2.5.3 EURODAC

The EURODAC system enables EU countries to identify asylum applicants as well as persons who have been apprehended in connection with an irregular crossing of an EU external border. EURODAC consists of a Central Unit within the Commission, equipped with a computerised central database for comparing fingerprints, and a system for electronic data transmission between EU countries and the database.

2.5.4 Second-generation Schengen Information System (SIS II)

The Schengen Information System (SIS) was initially established as an intergovernmental initiative under the Schengen Convention, before it was subsequently integrated into the EU framework. It is used by Schengen border guards and police as well as customs, visa and judicial authorities. SIS holds information on persons who have been involved in a serious crime or who do not lawfully reside in the EU. It also contains alerts on missing persons, in particular children, as well as information on certain property, such as banknotes, cars, vans, firearms and identity documents, that have been stolen, misappropriated or lost. Information is entered into the SIS by national authorities and forwarded via the Central System to all Schengen States.

On 9 April 2013, the second-generation Schengen Information System (SIS II) entered into operation. SIS II has enhanced functionalities, such as the possibility to use biometrics, new types of alerts, the possibility to link different alerts and a facility for direct queries on the system.

One of the world's largest IT systems in the field, SIS II consists of three components: a central ICT system, EU Member States' national ICT systems, and a network that links the systems.

2.5.5 Visa Information System (VIS)

The Visa Information System (VIS) enables Schengen countries to exchange visa data based on a centralised ICT system, which is linked to national ICT systems. VIS also

connects consulates in non-EU countries and all external border crossing points of Schengen States.

2.5.6 EU Operational Secure Wide Area Network (OPSWAN)

The EU Operational Secure Wide Area Network (OPSWAN) is a classified network that provides for coordination and command and control in CSDP missions. OPSWAN was created based on a Military CIS Concept for EU-led crisis management operations (Council of the European Union 2009). It is a networked solution to connect Brussels with potential HQs and other relevant actors such as the EU Satellite Centre (ESC). Its security is provided by the European External Action Service (EEAS) Communication and Information Systems (CIS) Directorate and the Network Defence Centre of the EU Council. OPSWAN connects Brussels (at the politico-military level) to Operational Head Quarters (OHQs) and the EU HQ at NATO Allied Command Operations (ACO) / Supreme Headquarters Allied Powers Europe (SHAPE). OPSWAN carries email, data, voice and fax traffic types. Several programmes and projects utilise the OPSWAN at the EU SECRET level.

2.5.7 European Union Command and Control Information System (EUCCIS)

The European Union Command and Control Information System (EUCCIS) provides functionalities at EU SECRET level relating to information management and exploitation capability for the EU Operations Centre (European External Action Service 2012). These enable operation commanders to effectively plan, monitor and conduct EU-led crisis management operations. EUCCIS encompasses the following functions:

- Email
- Access control and authorisation
- Logistical Functional Area Services
- Viewer – selection and viewing of GIS data to create the Common Operational Picture
- OPPFAS – Strategic Planning functionality similar in function to TOPFAS (Tamai 2009)
- Portal – web-based information exchange and collaboration platform to organise and manage information during an operation.

2.5.8 LOGFAS

Logistics Functional Area Services (LOGFAS) is a logistics management system that allows for the integration of those elements in the CSDP Command and Control structures contributing logistics support to an EU-led crisis management operation.

2.5.9 Military Intelligence Systems Support

These systems (primarily GIS related) help inform military intelligence appreciations for the planning and conduct of EU-led crisis management operations. As such, they have

unique requirements regarding the protection of sensitive and classified data whose compromise would jeopardise the ability of missions to achieve their objectives.

2.5.10 European Union Satellite Centre (EUSC)[3]

The European Satellite Centre (ESC) supports the work of the EEAS by providing geospatial imagery for CSDP and CFSP tasks. Data exchange with EU capitals is via the EU OPSWAN (EU Satellite Centre, 2012). Although positioned to support the EEAS and crisis management tasks of the European Union, the EUSC also offers capabilities in civilian domains including remote monitoring for scientific research.

2.5.11 COREU/CORTESY

The COREU/CORTESY network is a vitally important instrument of EU foreign policy, which in 2010 distributed nearly 8,500 messages on EU foreign policy to the (then) 27 Member States, the General Secretariat of the Council, and the European Commission.

2.6 Relevant security and privacy organisations within EU institutions and agencies

In this section we cover organisational structures having an inward-facing dimension for the governance, management or operations of cyber- and data security and data protection within the activities of EU institutions and agencies. We exclude, for example, DG HOME and DG JUST, which, although covering relevant areas, substantially do so in the context of their role of creating and monitoring implementation of policies in these areas in Member States.

2.6.1 Directorate-General for Informatics (DIGIT) (Brussels)

The mission of the Directorate-General for Informatics (DIGIT) is to enable the European Commission to effectively and efficiently use ICT in the course of achieving its organisational and political objectives. Towards this end, DIGIT is responsible for the:

- Definition of the European Commission's IT Strategy.
- Provision of IT infrastructure solutions and e-services, support services and telecommunications facilities to the Commission and other EU institutions and agencies.
- Delivery of information systems for EC corporate business processes.
- Promotion and facilitation of pan-European e-government services for citizens and enterprises.

[3] Council Joint Action 2001/555/CFSP of 20 July 2001 on the establishment of a European Union Satellite Centre amended by Joint Action 2006/998/CFSP, Joint Action 2009/834/CFSP and Council Decision 2011/297/CFSP.

In line with these mission objectives, DIGIT engages in two principal areas of activity. First, DIGIT provides the Commission as well as other European institutions and agencies with a secure and reliable high-performance ICT infrastructure. Secondly, DIGIT is responsible for the acquisition of ICT tools used within the Commission, the lifecycle management of ICT components, and the provision of support and training services related to the use of ICT equipment.

2.6.2 CERT-EU (Brussels)

Since 2011, DIGIT has been host to a permanent Computer Emergency Response Team (CERT-EU), which is supervised by the Director-General of DIGIT and steered by a group chaired by the Council. CERT-EU's task is to support EU institutions and agencies in their fight against cyber threats. Towards this end, CERT-EU engages in information-sharing, threat assessment and awareness-raising activities.

2.6.3 EU Council Network Defence Centre (Brussels)

In 2010, the General Secretariat of the Council of the EU launched the Network Defence Centre (NDC). Its objective is to strengthen the protection of EU sensitive and classified Communication and Information Systems against all forms of technical attacks, including Advanced Persistent Threats, through the development of the capability to detect and respond to security incidents.

2.6.4 Security Operations Centres (SoC) – DIGIT (Luxembourg)

The DIGIT Security Operations Centre (SOC) is managed by a Local Information Security Officer (LISO) who also acts as an advisor to the Information Security Steering Committee. The LISO analyses the security requirements of DIGIT's ICT systems and proposes policies that govern the ICT systems in line with the latter's needs.

2.6.5 European Agency for the operational management of large-scale IT systems (Tallinn)[4]

The European Agency for the operational management of large-scale IT systems became fully functional on 1 December 2012 and has since been responsible for the operational management of IT systems in the area of home affairs. Specifically, the Agency manages aspects related to the technical use of SIS II (Article 3), VIS (Article 4) and EURODAC (Article 5).

The Agency's core task is to ensure the uninterrupted exchange of data between national authorities (Article 7(3)). However, the Agency is also responsible for adopting and implementing security plans to prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or transport of data media. These security plans focus in particular on implementing appropriate encryption

[4] Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

techniques. Indeed, the Agency is to ensure that no system-related operational information circulates in the communication infrastructure without encryption.

The Agency is envisaged to evolve eventually into an EU Centre of Excellence for the development and operational management of other future systems in the policy domain of home affairs.

2.6.6 European Data Protection Supervisor (EDPS)[5]

A European Data Protection Supervisor (EDPS) as well as an Assistant Supervisor and an institutionally independent supporting structure were established in January 2004 (Chapter V). The EDPS's mission is to ensure that EU institutions and agencies respect individuals' fundamental rights and freedoms, specifically their right to privacy, when processing personal data or developing new policies (Article 41(2)).

Towards this end, the EDPS has a variety of duties, including:

- Hearing and investigating complaints by data subjects.
- Conducting enquiries either on his or her own initiative or on the basis of a data subject's complaint.
- Monitoring and ensuring the implementation of Regulation (EC) No 45/2001 and any other EU legislation related to the processing of personal data by an EU institution or agency.
- Advising EU institutions and agencies on all matters concerning the processing of personal data, specifically when they draw up internal rules related to the protection of fundamental rights and freedoms with regard to the processing of personal data.
- Monitoring developments that have an impact on the protection of personal data, specifically when they relate to ICT developments (Article 46).

To meet these responsibilities, the EDPS enjoys several competences and powers, including the right to:

- Give advice to data subjects in the exercise of their rights.
- Make proposals for improving the protection of data subjects.
- Order that requests to exercise certain rights in relation to data be complied with.
- Order the rectification, blocking, erasure or destruction of all personal data that have been processed in breach of the provisions governing the processing of personal data.
- Impose a temporary or definitive ban on the processing of personal data.
- Intervene in actions brought before the Court of Justice.

[5] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

- Obtain access to all personal data and to all information necessary for his or her enquiries.
- Obtain access to any premises in which an activity covered by Regulation (EC) No 45/2001 is being carried out (Article 47).

The EDPS is also party to the Article 29 Working Party, which is otherwise composed of representatives of national data protection authorities and the European Commission. The main tasks of the Article 29 Working Party, which was set up under Directive 95/46/EC,[6] are to:

- Provide expert advice from the national level to the European Commission on data protection matters.
- Promote the uniform application of Directive 95/46 in all Member States of the EU, as well as in Norway, Liechtenstein and Iceland.
- Advise the Commission on any EU legislation that affects the right to protection of personal data (Article 29).

2.7 Conclusion

As has been shown, there is a complex mix of business requirements for the use of ICTs by EU institutions and agencies. These requirements are made up not only of internally focused activities such as procurement, HR, finance and accounting but also a complex set of outward-facing systems and requirements that support either policies or, in the case of ASFJ and CSDP, direct operational intervention in certain areas.

The move to BYOD or the use of cloud computing by EU institutions and agencies follows the path of other public sector bodies: it is possible to discern a very cautious approach, but there clearly is a certain inertia that comes with an entity of around 50,000 employees spread over numerous institutions and geographical locations.

Viewed differently, however, the scale of some EU wide activities (e.g. the processing of large amounts of nominal data by SIS II or the sharing and management of law enforcement intelligence contributed by many Member States coordinated by Europol), and the management of highly sensitive classified information in EU-led CSDP and crisis management operations as well as some other areas, imposes some especially unique requirements that act as inhibitors when it comes to the rapid adoption of cloud computing, BYOD, or other innovative IT developments seen in other contexts.

At the same time, like many other national and international public bodies, EU institutions and agencies are faced with many diverging pressures regarding ICT provision, such as:

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- The demand for efficiency in a time of austerity, pushing or encouraging the adoption of cloud computing or 'software as a service' solutions.
- Business demands for mobility, including not only calls for remote access but also the drive to seamless shifting between personally owned and corporately provided IT devices.
- The evolving threat landscape, which is currently dominated by the Advanced Persistent Threats (APT) and, to a growing extent, concerns over government surveillance.
- Increasing societal expectations concerning e-democracy, transparency and respect for human rights, such as the right to the protection of personal data.

3. Cross-cutting legal and policy frameworks applicable to EU institutions and agencies

In this Chapter we summarise the main cross-cutting frameworks governing data and information handling in relation to topics of direct relevance to this study, namely security of (unclassified and classified) systems, data protection and document management. We find that:

- Cybersecurity legal and policy frameworks applicable to EU institutions and agencies consist of Regulations, Decisions, Rules, Policies and Guidance, with each imposing decreasing levels of obligation.
- The main EU Regulation governing data protection matters dates from 2001 and is based on the 1995 EU General Data Protection Directive 95/46/EC,[7] which itself is currently under review.
- The overall tone of EU policy and legal frameworks governing and regulating information security resonates with a model of security based on an internally secure organisation and insecure external environment, which appears to be inconsistent with the latest evolving canon of best practice concerning inter-organisational security, as, for example, codified by the International Standards Organisation.
- Key EU information security and data protection frameworks would appear poorly aligned with many modern models of technology service delivery and use, including cloud computing, the consumerisation of IT (BYOD), service-orientated architectures (SoA), and an open model of IT services mediated through cyberspace. For example, although the e-Commission Communication flags up the involvement of the European Commission in the Cloud Computing Strategy, it is not clear that existing security frameworks are also aligned.

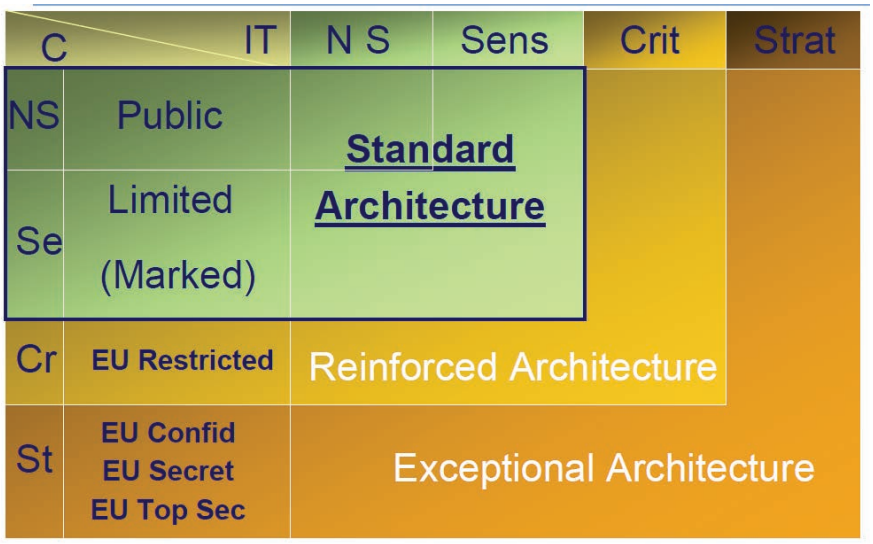
[7] Directive 95/46/EC is the reference text, at EU level, on the protection of personal data. It defines a regulatory framework that seeks to strike a balance between the protection of individual privacy and the free movement of personal data within the EU. To this end, the Directive defines limits to the collection and use of personal data and demands that each Member State set up an independent national body responsible for the protection of personal data.

- The potential for security and privacy requirements to be built in from the start through Security Engineering or Privacy by Design principles appears to have little visibility in many of the EU legal and policy frameworks this chapter covers.

3.1 General data and information handling

Figure 3.1 below outlines the European Commission's general model of information security, which informs several of the EU data and information handling policy and legal frameworks and corresponding organisational structures discussed in this section.

Figure 3.1: European Commission security architecture



NS: Not Secret information; Sens: Sensitive information;
Critical: Critically important information; Strat: Strategically important information.

Source: Moran (2010)

3.1.1 Commission Decision C(2006) 3602 of 2006[8]

Commission Decision C(2006) 3602 constitutes the main framework document on security measures and organisational guidelines for the protection of the Commission's information systems and the information processed therein (Article 1 (1)). However, the security measures and organisational guidelines defined in the Decision are applicable to a broad range of EU institutions and agencies, specifically:

- All European Commission DGs and Departments
- The Joint Research Centre
- EU delegations in third countries
- Offices with administrative links to the Commission

[8] Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission.

- All Executive Agencies using the Commission's information systems
- Persons under contract to the Commission and subcontractors who have access to and use the Commission's information systems (Article 2).

As regards the stipulation of specific information security measures, the Decision primarily covers the use of encryption technologies (Article 6), responses in the case of security incidents (Article 7), and the general security capabilities of information systems (Article 8). The latter are to be determined in line with the security needs of information systems and those of the information they process (Annex 1(C1)). Thus, the Decision distinguishes between 'standard' information systems where the security requirements are met by the security measures provided by the basic infrastructure of the Commission's information systems, and 'specific' information systems, where the security requirements make it necessary for additional security measures to be put in place (Annex 1(C2)).

Also addressing organisational aspects, the Decision clarifies that, on a vertical level, the individual DGs and their Departments and, on a horizontal level, the Security Directorate within DG Human Resources (DG HR) as well as DIGIT are responsible for ensuring information system security across the EU's ICT infrastructure.[9] Specifically, the individual DGs and Departments are responsible for drawing up, implementing, and managing security plans for their ICT systems as well as for defining guidelines, human resources, budgetary resources, and IT resources for their ICT-related activities (Annex II(A)). Notably, DGs may delegate all or part of the implementation and management of their security plans to horizontally operating entities, Departments such as DIGIT.

Pursuing a horizontal oversight function, the DG HR Security Directorate is responsible for coordinating all activities relating to the implementation the Decision and for ensuring that activities carried out under the Decision are consistent with EU ICT security policy standards (Annex II(I)). Moreover, the DG HR Security Directorate organises training, awareness-raising and support activities in cooperation with the Departments in charge of general and ICT training at the Commission, and it assists DGs in the implementation of the relevant ICT security policy standards. Finally, the DG HR Security Directorate ensures that ICT security policy standards are taken into account when DIGIT and the other DGs draw up IT strategies.

On a more technical level in the horizontal domain, DIGIT is responsible for ensuring the security of the Commission's private electronic communications network and the network for the Commission's external sites, contractors and all authorised partners (Annex II(J)). DIGIT further provides architecture blueprints, reference configurations, and IT software, which satisfy the EU's ICT security policy standards. At the same time, DIGIT draws up and implements a programme of measures to prevent the exploitation of vulnerabilities in Commission ICT systems, and it also manages the general security mechanisms, such as firewalls, intrusion detection programmes, antivirus programmes, or authentication systems. Last but not least, DIGIT is supposed to manage security incidents in cooperation with the DG HR Security Directorate.

[9] Anonymous interviewee, 3 March 2014.

Individual DGs and Departments are also subject to further security oversight from Local Informatics Security Officers (LISOs). Appointed within each DG, LISOs are independent of the information system security management within the DG and responsible for monitoring the implementation of systems security as well as ensuring that their DG is kept abreast of relevant developments in IT-related security. Beyond ensuring implementation, LISOs constitute first line of response when it comes to detecting and responding to attacks on their DG's ICT systems (Annex II(B)).

3.1.2 Implementing rules for Commission Decision C(2006) 3602 of 2006

The implementing rules for Decision 3602 allow the updating of either standards (obligatory) or guidelines (voluntary). An example that is relevant to the issues over security specifically (especially with regard to BYOD) is a Standard from 2010 on Logging and Monitoring.

European Commission Security Standard on Logging and Monitoring (2010)[10]

Drawn up by the Security Directorate and adopted by the Director-General of DG HR in 2010, the European Commission Security Standard on Logging and Monitoring (SSLM) supplements Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission (para. 1). Rooted in three international norms, namely ISO/IEC 27001 (second edition of 15/06/2005), ISO/IEC 17799 (second edition of 15/06/2005), and the NIST SP 800-92 Guide to Computer Security Log Management, SSLM provides mandatory instructions for the procedures to be used for logging and monitoring on all ICT systems that are capable of generating information security-related log events (para. 3), including but not limited to:

- Servers
- Workstations
- Portable PCs
- Other portable computing devices, such as mobile phones and PDAs
- Storage devices
- Network equipment (para. 4).

Security controls defined in the SSLM are aimed at reducing the threat emanating from a wide range of information security incidents:

- Loss of power supply
- Failure of telecommunication equipment
- Tampering with hardware
- Tampering with software
- Equipment failure

[10] SEC20.10.05/04 – Standards.

- Equipment malfunction
- Saturation of the information system
- Software malfunction
- Unauthorised use of equipment
- Corruption of data
- Illegal processing of data
- Error in use
- Abuse of rights
- Forging of rights
- Denial of actions (para. 5).

The Commission SSLM provides a comprehensive list of required logging practices with regard to individual device types (para. 8.2.). The EC's applications and network environments must be monitored to ensure that threats are identified and alerts must be raised promptly (para. 9.1.).

Specifically, this standard stipulates that the following systems must be monitored:

- Firewalls (both network and host-based)
- Any other gateways to other networks
- Intrusion detection / prevention systems
- Authentication servers.

The SSLM stresses that all monitoring systems must have the capability to aggregate and analyse information security incidents affecting multiple systems. Alerts must be sent automatically to system administrators so that they can react to potential threats.

Events monitored must include at least the following:

- Unauthorised access attempts, such as failed or rejected user logins or other actions or critical notifications from network firewalls or gateways such as dropped traffic or specific rules (e.g. firewall management rules).
- System alerts or failures such as console alerts or messages, system log exceptions, network management alarms, alarms raised by the access control system, system capacity alerts, or Key Performance Indicators.
- Changes to, or attempts to change, system security settings or controls.

It stresses that particular attention should be paid to the monitoring of systems that have been infiltrated, compromised or misused in the past, and to systems that are exposed to high risks (for example, systems that can be reached from the Internet).

3.1.3 Council Decision 2013/488/EU on the Security Rules for Protecting EU Classified Information

Council Decision 2013/488/EU sets out basic principles and minimum standards for protecting EU Classified Information (EUCI) (Article 1(1)), including provisions on processing EUCI through ICTs. The Decision applies to the handling of EUCI by a wide range of EU institutional actors, specifically:

- The Council, Council preparatory bodies, and the Council Secretariat
- The Commission
- The European External Action Service (EEAS), Common Foreign and Security Policy (CFSP) agencies and bodies, EU Special Representatives, and EU crisis management operations personnel
- Europol and Eurojust.

The European Parliament as well as all other EU agencies and bodies are associated with the rules when necessary (Article 1(4-8)).

EU Member States, their contractors and sub-contractors are also expected to respect the Decision's rules and procedures when handling EUCI (Article 1(3)), without, however, impeding upon national parliaments' right of oversight (Article 1(11)).[11]

The Council Decision stipulates two overarching requirements for ensuring the effective protection of EUCI processed through ICTs. First, all ICTs handling EUCI have to provide appropriate levels of Information Assurance (IA). The Council's understanding of IA encompasses five concepts:

- Authenticity, i.e. the guarantee that information is genuine and from bona fide sources.
- Availability, i.e. the property of being accessible and usable upon request by an authorised entity.
- Confidentiality, i.e. the property that information is not disclosed to unauthorised individuals, entities or processes.
- Integrity, i.e. the property of safeguarding the accuracy and completeness of information and assets.
- Non-repudiation, i.e. the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied (Annex IV, paragraph 2).

Secondly, security risk management is to inform the definition, development, operation and maintenance of all ICT (Annex IV, para. 4). Security risk management is conceived of as an iterative process among system owners, project authorities, operating authorities and security approval authorities, which entails assessment, treatment, acceptance and

[11] The Decision commits Member States to ensure that contractors and sub-contractors registered in their territory undertake the measures necessary to protect EUCI both during contractual negotiations and when delivering on a contract (Article 11 (4)).

communication of risks. The Council has underlined that security risk management should strike a satisfactory balance between user requirements, costs and residual security risk (Annex IV, para. 6).

As part of its efforts to meet Information Assurance and security risk management requirements, the Council aims at the cultivation of a range of technical and non-technical security measures. These measures can be grouped into five thematic areas:

- Deterrence, i.e. the dissuasion of any adversary planning to attack ICTs
- Prevention, i.e. the blocking of an attack on ICTs
- Detection, i.e. the discovery of an attack on ICTs
- Resilience, i.e. the limitation of negative effects of an attack on information or ICT assets and the prevention of further damage
- Recovery, i.e. the reestablishment of a secure situation for ICTs.

The majority of security measures implemented within these five areas are to be defined in separate IA security policy documents and guidelines (Annex IV, para. 3), based on advice from a Security Committee, which is composed of Member State representatives and Commission and EEAS officials (Article 17(2)).[12] However, the Decision stipulates a range of baseline activities and procedures for ensuring the security of EUCI processed through ICT. These fall within four broad areas:

- Risk awareness and preparedness and information access control
- ICT installation and lifecycle management
- ICT Interconnectedness
- Electronic transmission of EUCI.

To increase risk awareness and preparedness, personnel handling EUCI are expected to receive regular training on identifying potential risks to ICTs and on applying the security measures in place to mitigate these risks (Annex IV, para. 21). At the same time, the application of a 'principle of least privilege', which ensures that ICT users and automated processes are only given the access, privileges and authorisations necessary for performing their assigned tasks, is expected to further reduce potential vulnerabilities on the human resources side.

The Council has decided that ICTs handling EUCI can only be installed in areas that are subject to appropriate physical security measures (Article 8(3)). All ICTs processing EUCI are to be built in line with a 'principle of minimality' (Annex IV, para. 18-19), i.e. only those functions, devices and services that are vital to meeting operational requirements are built into them. Furthermore, they need to undergo an elaborate accreditation process to verify that appropriate security features have been implemented (Article 10(4)). Such

[12] The Security Committee can also recommend annual assessments of the performance of Member State bodies as well as EU institutions and agencies operating within the remits of the Decision (Article 16 (1c)). In its activities, the Security Committee is supported by an expert group on IA and additional expert groups as necessary (Article 17 (3)).

features include TEMPEST measures, which protect EUCI data against unintentional exposure to electromagnetic emanations (Article 10(5)).

To ensure appropriate levels of EUCI security throughout an ICT's lifecycle, the Council envisages regular inspections and reviews of ICT components (Annex IV, para. 11) and constant updating of relevant security documentation (Annex IV, para. 12). In addition, the General Secretariat of the Council and the Member States are expected to cooperate on developing best practices for handling EUCI on ICTs (Annex IV, para. 13).

With regard to the interconnection of ICT, the Council stipulates that all ICTs processing EUCI shall treat other ICTs as untrusted by default (Annex IV, para. 33). More specifically, the Council rules out any interconnection between an accredited ICT and an unprotected or public network, except where an ICT handling EUCI has Boundary Protection Services specifically installed for such a purpose. The security measures for such interconnections shall be reviewed by the competent Information Assurance Authority (IAA) and approved by the competent Security Accreditation Authority (SAA). However, any cascaded interconnection of an ICT accredited to handle EU TOP SECRET to an unprotected or public network is prohibited. Notably, the usage of an unprotected or public network as a carrier for data that is encrypted by an approved cryptographic product is not considered an interconnection.

Within secured areas or administrative areas, the transmission of EUCI can take place on an unencrypted or lower-level encryption basis (Annex IV, para. 31). For the transmission of EUCI outside of physically protected areas, the Council has identified cryptographically protected electronic transmission as the medium of choice (Article 9(4a)). However, the Council also allows for the usage of cryptographically protected physical media, such as memory sticks, hard drives or DVDs (Article 9(4bi)).

Cryptographic products used for protecting EUCI are, in the first instance, evaluated and approved by a Member State Crypto Approval Authority (CAA) (Annex IV, para. 25). Subsequently, a second party evaluation is carried out by the CAA of another Member State, which has not been involved in the design or manufacture of the equipment (Annex IV, para. 26). Cryptographic products, which protect EUCI classified as SECRET and TOP SECRET, require final approval by the Council before they can be used within EU institutions and agencies and/or Member States. Cryptographic products that protect EUCI classified as CONFIDENTIAL and RESTRICTED require approval by the Secretary-General of the Council or by Member States on the national level (Article 10(6)). By way of derogation from standard procedure, the Council or the Secretary-General of the Council can, on the recommendation of the Security Council, approve cryptographic products on an interim basis without prior evaluation by a Member State CAA (Annex IV, para. 27). Likewise, upon recommendation by the Security Committee, the Council can accept the evaluation of cryptographic products by third states or international organisations for EUCI released to the evaluating third state or international organisation.

Significantly, the Council has formulated a general caveat with regard to the electronic transmission of EUCI to third states or international organisations. Thus, any exchange of EUCI with third states or international organisations shall take place by means of a physical medium, unless a security of information agreement (Annex VI, para. 7) or an

administrative arrangement (Annex VI, para. 21) explicitly provides for electronic transmission. Similarly, in the context of CSDP missions, an express permission for the electronic exchange of classified information needs to be stipulated within a framework participation agreement, an ad hoc participation arrangement, or an ad hoc administrative arrangement (Annex VI, para. 27).

3.1.4 Commission Decision 2001/844/EC, ECSC, Euratom

Commission Decision 2001/844/EC, ECSC, Euratom defines security measures aimed at protecting EU institutions and agencies against unauthorised disclosure of EUCI (i.e. the loss of confidentiality) and against the loss of integrity and availability of such information (para. 25.1.3.). The Decision informs and, at the same time, supplements Council Decision 2013/488/EU. Indeed, most of the security measures specified in Commission Decision 2001/844/EC, ECSC, Euratom are more or less analogous to the rules and procedures stipulated in Council Decision 2013/488/EU.

However, some of the Commission Decision's rules and guidelines are not or only superficially covered by Council Decision 2013/488/EU. These relate to three areas:

- The logging of EUCI processed through ICT systems
- The use of contractor-owned or nationally supplied IT equipment for official Commission work
- The use of privately owned IT equipment for official Commission work.

The Decision stipulates that any access to information classified as SECRET and above must be logged automatically or manually. Similarly, any output generated by a system handling EUCI and transmitted to a remote terminal/workstation area from an IT area needs to be logged. The Decision highlights that for SECRET and above such procedures need to include specific instructions for accountability of the information (para. 25.5.2.).

According to the Decision, the use of contractor-owned IT equipment and software in support of official Commission work must be permitted by the Director of the Security Directorate. The use of nationally-provided IT equipment and software is possible only when brought under the control of the appropriate Commission inventory. In either case, the Decision stipulates that any IT equipment used for handling EUCI must be evaluated in terms of its information security capabilities (para. 25.8.3.).

The Decision highlights that no privately owned removable computer storage media, software or IT hardware, such as PCs, notebooks or tablets, may be used for processing EUCI. Moreover, privately owned hardware, software or media may not be brought into any area where EUCI is handled without the written authorisation of the Director of the Security Directorate, which can only be provided for exceptional technical reasons (para. 25.8.2.).

3.1.5 Regulation (EC) No 45/2001 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data

Regulation (EC) No 45/2001 imposes a set of obligations on data controllers within EU institutions and agencies with regard to handling personal data of employees and other affected data subjects (Preamble, para. 5 & 7) in order to protect the privacy of these data subjects (Article 1). In line with this overarching aim, the Regulation stipulates, in the first instance, that EU institutions and bodies are only allowed to collect personal data that serves specified, explicit and legitimate purposes. The data collected have to be adequate, relevant and not excessive when evaluated against the collection purpose, as well as accurate and up to date. Furthermore, the personal data collected may not allow for the identification of data subjects for a period longer than absolutely necessary for pursuing the purposes for which the data was initially collected (Article 4(1)).

Significantly, several types of ICT communication data are explicitly excluded from the list of legitimately collectable private data. Indeed, the Regulation stipulates that EU institutions and agencies have to ensure the confidentiality of communications by means of telecommunications networks and terminal equipment, in accordance with the relevant EU legislation (Article 36). User traffic data that is processed and stored to establish calls and other connections over the telecommunications network have to be erased or anonymised upon termination of the call or connection (Article 37(1)).[13] Moreover, the amount of personal data contained in electronic user directories should not exceed what is strictly necessary for the specific purposes of the directory (Article 38).

The Regulation not only imposes certain obligations with regard to the collection of personal data but also with regard to the processing of such data. Thus, EU institutions and agencies may only process personal data when the data subject has given his or her consent or else:

- For the performance of a task carried out in the public interest, in accordance with relevant EU legislation or in the legitimate exercise of official authority vested in an EU institution or agency or in a third party to whom the data are disclosed.
- For compliance with the data controller's legal obligations.
- For the performance of a contract the data subject is a party to or in order to take steps at the request of the data subject prior to entering into a contract.
- To protect the vital interests of the data subject.

Limitations in the amount of personal data collected and conditions under which it can be processed are a function of security considerations. Addressing both physical and electronic data processing operations, the Council and the European Parliament have identified four operations they consider to pose particular challenges with regard to protecting the privacy of data subjects:

[13] However, traffic data may be processed for the purpose of budget and traffic management, also including the verification of authorised use of the telecommunications systems (Article 37 (2)).

- The processing of data related to health, suspected offences, offences, criminal convictions or security measures.
- The processing of data pertaining to professional or personal qualities of the data subject, including his or her ability, efficiency and conduct.
- Processing operations allowing data set linkages not in accordance with national or EU legislation.
- Processing operations for the purpose of excluding individuals from rights, benefits or contracts (Article 27(2)).

However, the Regulation only rules out the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and of personal data concerning health or sex life (Article 10). Derogations are limited to cases where:

- The data subject has given his or her express consent and the expression of such consent is in accordance with the internal rules of the EU institution or body processing the data.
- The data controller has to comply with specific employment law rights and obligations, in accordance with relevant EU legislation.
- The vital interests of the data subject are at stake.
- The data has been manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.
- The data processing is carried out by a non-profit-seeking entity within an EU institution or agency that has a political, philosophical, religious or trade union aim (Article 10(2)).
- The data are used for the administering of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of health care services, and the data are processed by a health professional or by another person who is also subject to professional secrecy (Article 10(3)).
- The data are used in relation to offences, criminal convictions or security measures carried out in accordance with relevant EU legislation (Article 10(5)).

In addition to addressing the processing of personal data, the Regulation also touches upon the privacy implications of transferring personal data. In this context, the Regulation defines three legal categories of personal data transfer:

- Within or among EU institutions and bodies (Article 7).
- To recipients in EU Member States and in other states, which are subject to Directive 95/46/EC, such as European Economic Area countries (Article 8).
- To recipients not subject to the Directive (e.g. organisations or companies established in countries without data protection legislation or with legislation that does not meet the Directive's protection standard) (Article 9).

Within or among EU institutions and agencies, personal data can be transferred to any data recipient who claims to perform legitimate tasks that fall within the remit of his or her competencies. In contrast, any transfer of personal data to recipients in EU Member States and in other states, which are subject to Directive 95/46/EC, requires prior production of proof by the data recipient that the data requested is necessary for performing a task carried out in the public interest or on public authority grounds. However, with such personal data transfers Member States should not negatively affect the data subject's legitimate interests.

Recipients that are not subject to Directive 94/46/EC (including some international organisations) have to prove that they are able to provide adequate levels of data protection before they can receive information from EU institutions or agencies (Article 9(1)). The EU establishes the adequacy of protection on the basis of five criteria:

- The nature of the data to be protected.
- The purpose and duration of the proposed data processing operation or operations.
- The recipient third country or recipient international organisation in question.
- The relevant legislation in force in the third country or international organisation in question.
- The professional rules and security measures that are complied with in the third country or international organisation (Article 9(2)).

However, even in cases where third states or international organisations do not or only insufficiently meet the criteria, personal data can be transferred when the data subject has given his or her consent or the transfer is related to a contract between the data subject and the controller or a contract between the controller and a third party that is in the data subject's interest. Personal data can also be transferred to serve important public interests or to protect the vital interests of the data subject (Article 9(6)).

Acknowledging the level of risk to privacy inherent in processing and transferring personal data, the Regulation commits data controllers to implement technical security measures that are commensurate with the sensitivity of the personal data in question (Article 22(1)). The aim of these measures is to first and foremost:

- Prevent any unauthorised person from gaining access to computer systems processing personal data.
- Prevent any unauthorised reading, copying, alteration or removal of storage media.
- Prevent any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data.
- Prevent unauthorised persons from using data-processing systems by means of data transmission facilities.
- Ensure that authorised users of a data-processing system can access no personal data other than those to which their access right refers (Article 22(2)).

Resonating with the aim of implementing appropriate technical security measures, the Regulation explicitly stipulates the need to monitor ICTs processing personal data in order to protect such data from becoming subject to unauthorised access (Preamble, para. 30). Specifically, EU institutions and agencies are required to take appropriate technical and organisational measures to safeguard the secure use of telecommunications networks and terminal equipment. To this end, they are expected to closely coordinate with the providers of publicly available telecommunications services or the providers of public telecommunications networks where appropriate. Taking into account the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented (Article 35(1)). In the event of any particular risk of a breach of the security of the network and terminal equipment, the EU institution or agency concerned shall inform users of the existence of that risk and of any possible remedies and alternative means of communication (Article 35(2)).

3.1.6 Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents

Regulation (EC) No 1049/2011 defines principles, conditions and limits governing the right of access to European Commission, Council and European Parliament documents (Article 1(a)). The Regulation also sets out a range of measures aimed at promoting good administrative practices with regard to access to EU documents (Article 1(c)). The Regulation applies to all documents drawn up, received by or in the possession of an EU institution or agency, regardless of the nature of the policy domain the documents cover (Preamble, para. 7).

The Regulation stipulates that EU documents are to be made accessible to the public in electronic form or through a register (Article 12(1)). This provision applies, in particular, to legislative documents, which are drawn up or received in the course of procedures for the adoption of legally binding acts (Article 12(2)). However, the Regulation also highlights that other documents, including policy or strategy documents, should be made directly accessible to the public (Article 12(3)).

At the same time, the Regulation also entails several caveats when it comes to making documents accessible to the public. Specifically, access to documents may not be granted where disclosure of these documents would negatively affect:

- The public interest as regards public security, defence or international relations, and the financial, monetary or economic policy of the EU or a Member State (Article 4(1a).
- An individual's privacy (Article 4(1b).
- A person's commercial interests.
- Court proceedings and legal advice.
- The purpose of inspections, investigations and audits (Article 4(2)).

In addition, the Regulation puts limits on the release of sensitive documents, which are defined as documents originating from EU institutions or agencies, Member States, third

countries, or international organisations, classified as TOP SECRET, SECRET or CONFIDENTIAL (Article 9(1)). Thus, sensitive documents are released only with the consent of the originator (Article 9(2)).

3.2 Emergent or proposed European Union legal and policy frameworks

In this section we cover some of the emerging or proposed legal initiatives that are likely to have a significant impact on the data protection and security aspects of future EU legal and policy frameworks.

3.2.1 European Commission proposal for a Directive ensuring a common and high level of Network and Information Security across the Union (NIS Directive)[14]

The presentation of the joint EEAS and European Commission EU Cyber Security Strategy in February 2013 was accompanied by another European Commission legislative proposal. The so-called 'NIS Directive' proposes a set of common standards and rules for ensuring a high level of Network and Information Security (NIS) across the Union. In this respect, the Directive defines various obligations for EU Member States and industry concerning cybersecurity capabilities and the reporting of broadly defined security incidents to competent authorities (CAs) and the public.

In an attempt to define security incidents, the Directive explicitly discusses the problem of personal data being compromised as a result of cybersecurity incidents (Preamble, para. 31). Accordingly, the Directive calls upon CAs and data protection authorities to cooperate and exchange information on all relevant matters related to tackling personal data breaches resulting from incidents. Moreover, CAs are expected to consult and cooperate with the relevant national law enforcement agencies and data protection authorities (Article 6(5)).

To live up to their mandate, CAs are expected to communicate via a secure network (using for example a secure pan-European electronic data exchange network, such as sTESTA) (Article 8(1)), which would allow them to:

- Circulate early warnings on risks and incidents
- Ensure a coordinated response
- Publish on a regular basis non-confidential information on on-going early warning and coordinated response (Article 8(3)).

The proposed NIS Directive also calls upon all EU Member States to set up CERTs that are able to handle incidents and risks (Article 7(1)), including those that affect the

[14] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of Network and Information Security across the Union

protection of personal data. Significantly, the Directive also stipulates that 'Member States shall ensure that CERTs have adequate technical, financial and human resources to effectively carry out their tasks' (Article 7 (2)) and defines the quality of such resources in some detail (Annex 1).

Moreover, public administrations and market operators are requested to notify incidents having a significant impact upon the security of the core services they provide to CAs (Article 14(2)). The latter can inform the public about the incident or require the disclosure of the incident to the public, if this is deemed to be in the public interest (Article 14(4)).

3.2.2 Proposal for a General Data Protection Regulation (GDPR)[15]

On 25 January 2012, the European Commission unveiled a draft legislative package to establish a unified European data protection law. The package also includes a proposal for 'General Data Protection Regulation' (GDPR), which will be directly applicable in all EU Member States. The Regulation is geared at updating and modernising the principles and rules stipulated in Directive 95/46/EC[16] and at streamlining the data protection laws currently in force in the different Member States, which have generally been aligned to the 1995 Directive.

Similarly to the 1995 Directive, the proposed Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data within the EU (Article 1(1)). However, the proposed new EU data protection regime extends much more explicitly to personal data handled by third-state data controllers (Article 41(1)). Indeed, the Regulation even applies to non-EU data controllers processing personal data of EU citizens, such as third-state companies and international organisations not physically represented within the EU (Article 40).[17]

At the same time, the Regulation also provides for an easier transfer of personal data outside the EU, including the transfer of personal data in clouds, when all data controllers involved commit themselves to specific corporate rules (Article 43). Under these rules, data controllers have a high degree of responsibility and accountability for the secure processing of personal data. For example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible and normally within 24 hours (Article 31). A harsh sanction regime applies when the Regulation's provisions are breached, allowing data protection authorities to impose penalties of up to 2 per cent of a company's worldwide turnover in case of misconduct (Article 79).

---

[15] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[16] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[17] While a similar rule is already present in Directive 95/46/EC, this rule defines a much more ambiguous criterion of equipment location, causing significant difficulties of interpretation and widespread non-compliance.

Concerning the rights of data subjects, the Regulation stipulates that any processing of personal data will require that the data subject is provided with clear and detailed information about the nature of the data processed (Article 14). Moreover, the data subject needs to gives his or her specific and explicit consent for the processing of personal data (an 'opt-in approach') (Article 6 (1a)). Unlike under the current Directive, the processing of the personal data of data subjects under the age of 13 always requires parental consent, which will make it more difficult for companies to conduct business with minors.

The Regulation also introduces the data subject's 'right of portability' and the 'right to be forgotten'. The right of portability allows the data subject to request for his or her data, such as email accounts, to be transferred from one electronic processing system to another without being prevented from doing so by the data controller (Article 18). The 'right to be forgotten' enables data subjects to request the unconditional erasure of all personal data and imposes an obligation on the data controller to inform third parties about the data subject's request for erasure of any copy or replication of that personal data (Article 17).

3.3 Relevant international standards and best practices

A considerable proportion of the legal and policy frameworks we have discussed in the preceding sections of this chapter are rooted in international standards and best practices. Accordingly, in this final section of Chapter 3 we cover some of the international soft law mechanisms that have informed EU legal and policy frameworks.

ISO2001 is probably the most commonly recognised and used set of standards regarding information security. This has been codified since the beginning of the 2000s from existing national standards such as BSI7799. It is understood[18] that much of the soft law guidance used by EU institutions and agencies is based on the ISO27000 suite of best practice but also that from ISACA and ITIL.

3.3.1 ISO Information Security Risk Management System (ISMS – 27001: 2008)

The suite of IT security technique documents represented by the ISO27000 series is an increasingly expanding canon of internationally accepted good practice concerning the management of information risk. The material is developed by an International Committee of the ISO/IEC JTC 1/SC 27 technical committee and now constitutes a series of 127 documents dealing with IT security in a variety of contexts. The ISO/IEC 27000 series has been acknowledged as a reference set of guidance for the management and organisation of information security (in and between organisations). Table 3.1 below lists the current set of reference documents.

Table 3.1: Overview of the ISO27000 suite

Title
27000 Information security management system (ISMS) – overview & definitions
27001 Information security management system – requirements

[18] Anonymous interviewee, 10 December 2013.

27002 Code of practice for information security controls
27003 Information security management system implementation guidance
27004 Information security management – measurement
27005 Information security risk management
27006 Requirement on bodies providing security audits
27007 Guidelines for information security management systems auditing
27008 Guidance for auditors on information security management system controls
27010 Information security management for inter-sector & inter-organizational communications
27013 Guideline on the integrated implementation of ISO/IEC 27001
27033 Network security
27034 Guideline for application security
27035 Security incident management

ISO/IEC 27001:2005 articulates a Plan-Do-Check-Act (PDCA) cycle of a process for management of information risks. ISO/IEC 27002:2013, based on the British Standard BS7799 provides a list of controls that can be applied to manage information risks. In the 2013 version of the original standard of 27002:2005, the controls are grouped into the following areas:

Table 3.2: Headings in ISO27002:2013

Heading	Sub headings
Information security policies	Management direction for information security
Organization of information security	Internal organization, Mobile devices and teleworking
Human resource security	Prior to employment, During employment, Termination and change of employment
Asset management	Responsibility for assets, Information classification, Media handling
Access control	Business requirements of access control, User access management, User responsibilities, System and application access control
Cryptography	Cryptographic controls
Physical and environmental security	Secure areas, Equipment
Operations security	Operational procedures and responsibilities, Production from malware, Backup, Logging and monitoring, Control of operational software, Technical vulnerability management, Information systems audit coordination
Communication security	Network security management, Information transfer
System acquisition, development and maintenance	Security requirements of information systems, Security in development and support processes, Test data
Supplier relationships	Information security in supplier relationships, Supplier service delivery management
Information security incident management	Management of information security incidents and improvements
Information security aspects of business continuity management	Information security continuity, Redundancies
Compliance	Compliance with legal and contractual requirements, Information security reviews

There are a number of nationally and internationally developed tools or methods that allow the implementation of ISO27005. These include such methods as CRAMM (UK), EBIOS (FR) and MAGERIT (ES) (ENISA, n.d.).

3.4 Conclusion

This chapter has shown that there is a somewhat complex set of cross-cutting rules concerning data protection, information security, protection of classified information and transparency. There exist hard laws in the form of Regulations, Decisions (which apply only to the Commission), Standards, Policies (binding instruments that are not articulated in formal EU legislation) and Guidelines (non-binding instruments not articulated through formal EU legislation). This provides for a certain degree of flexibility, especially where Rules and Policies articulate objectives and guidelines can be developed specific to particular contexts.

The choice of a Regulation as an instrument to govern the protection of personal data is perhaps unsurprising given the nature of data protection as a fundamental right. Nonetheless, we can identify some challenges pertinent to these frameworks when we consider the adoption of new technologies.

There would appear to be an implicit perimeter-based model of security in the various policy frameworks. This is understandable given the trusted nature of EU institutions and agencies as examples of large public administrations where those non-sensitive functions that are outsourced are performed by a small number of contractors. However, in other domains, the model of outsourcing and the perimeter-less enterprise has become more prevalent, especially with the service-led economy, where it is not easy to determine who or what processes are provided externally or internally. If EU institutions and agencies are to try further to drive efficiencies through making use of outsourcing or service-orientated architectures, a more sophisticated set of frameworks will need to be put in place to cope with these models.

Regulation 45/2001 is very much based on the General Data Protection Directive 95/46/EC. As such, it remains to be seen whether it will be sufficient in articulating the right to the protection of personal data in a modern context of cloud computing, blurred distinctions between data controllers and data processors, and a number of other challenges. Indeed, these challenges have become so pressing that the basis document 95/46/EC is in itself undergoing a process of reform, with new rules being proposed in 2012. It is unclear at this time whether the legal framework governing data protection within the work of EU institutions and agencies will be updated in line with the 2012 Commission Proposals for a new legal framework governing privacy and data protection. Similarly, there are other gaps where legal mandates make little provision, including such concepts as privacy or security by design and privacy-enhancing technologies (PETs).

Turning to information security, the use of the ISO27000 suite of guidance on information security management, including the Plan-Do-Check-Act cycle, is also unsurprising. However, it is unclear to what extent implementing guidance takes account

of the evolutions in the ISO27000 standard, particularly as it relates to inter-organisational security and the development of specific frameworks covering good practice on, for example, incident management.

On a related note to the question of security by design, the current frameworks governing the protection of EUCI (Council Decision 2013/488/EU) appear to pay little attention to evolving concepts of, for example, inter-domain security and more sophisticated audit and accountability that necessarily goes along with security governance concerning sensitive and protectively marked information.

Finally, although we have seen in Chapter 1 that adoption of cloud computing technologies is very much on the e-Commission agenda, there appears to be little recognition of this in the security and privacy policy and governance frameworks as applied to EU institutions and agencies. As work from ENISA has shown, the establishment and adoption of risk management frameworks that take account of the intricacies of cloud computing for certain use cases (e.g. the public sector) is extremely important. At the enterprise level, evolution in the Information Security Management System frameworks would need to take account of the complex joint and several allocation of responsibilities for security between the cloud service provider and the cloud service user (in this case, for example, the European Commission). Furthermore, the specific aspects of cloud computing relating to data protection, namely transparency, consent and accountability, would need to be addressed in any updated data protection framework that would apply to EU institutions and agencies.

4. Legal and policy frameworks covering policy domains unique to EU institutions and agencies

In Chapter 4 we explain some key aspects of building blocks relating to activities that, due to their scale, complexity or domain are unique to the EU. These include:

- The internal market (for example, transportation, emissions trading, services provision or civil nuclear energy).
- Justice and home affairs (covering police and law enforcement cooperation, customs, asylum and border security).
- The Common Foreign and Security Policy (CFSP), encompassing data exchange systems for foreign affairs, and operational command and control of EU-led CSDP missions.

By mapping legal and policy frameworks, which cover policy domains that are unique to EU institutions and agencies, such as the management and processing of sector-specific data, the processing of personally identifiable nominal data for intelligence, border management and criminal justice cooperation, or the processing of sensitive classified information for EU-led crisis management operations, we find that that:

- There is a complex landscape of very specific information security and data protection requirements for different EU policy domains.
- The unique nature of some of these policy domains and their attendant security or privacy considerations seem difficult to reconcile with the appetite for more innovative types of technology provision (e.g. through greater consumerisation of corporate IT assets or greater use of cloud computing).
- Understanding information security governance and data protection remains a challenge within many EU frameworks, which are often managed in a federated fashion through obligatory standards and rules set at a strategic EU level (either through the EU Council or Council of Europe) and implementation at the national level.

4.1 Specific legal frameworks covering the operation of the internal market

In this section we describe some specific security and privacy frameworks relevant to the operation of the internal market. These have been built upon business uses for ICT that exist in addition to those covered in Chapter 3.

4.1.1 Cross-border payments within the EU

Payment Services Directive (PSD)[19]

The Payment Services Directive (PSD) provides the legal foundation for the creation of a single market for payments in the EU. The target is to make cross-border payments as easy, efficient and secure as 'national' payments within a Member State. The PSD also seeks to improve competition by opening up payment markets to new entrants, thus fostering greater efficiency and cost reduction. At the same time the Directive provides the necessary legal platform for the Single Euro Payments Area (SEPA).

The Directive calls upon Member States to permit the processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, investigation and detection of payment fraud. Notably, the processing of such personal data is to be carried out in accordance with Directive 95/46/EC (Article 79).

Significantly, the Directive does not apply to services provided by technical service providers, which support the provision of payment services, without entering at any time into possession of the funds to be transferred. Such services may include:

- The processing and storage of data
- Trust and privacy protection services
- Data and entity authentication
- ICT network provision
- The provision and maintenance of terminals and devices used for payment services, with the exclusion of payment initiation services and account information services (Article 3(j)).

[19] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC Text with EEA relevance.

European Commission Proposal for a Revised Payment Services Directive (PSD II)[20]

The proposed Directive recognises that since the adoption of the 2007 PSD new types of payment services have emerged in the area of Internet payments. Specifically, PSD II refers to third-party providers (TPPs), which offer payment initiation services to consumers and merchants, often without entering into the possession of the funds to be transferred. Those services facilitate e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the consumer in order to initiate Internet payments on the basis of credit transfers or direct debits. In this respect, the proposed Directive highlights that TPPs are not always following the requirements of the PSD, raising a series of legal issues, such as consumer protection, security and liability, as well as competition and data protection issues (Preamble, para. 18).

The proposed Directive therefore highlights that it is necessary to set up the criteria under which TPPs are allowed to access and use information on the availability of funds in the payment service user account held with another payment service provider. In particular, necessary data protection and security requirements set or referred to in this Directive or included in the European Banking Authority guidelines should be fulfilled by both the TPP and the payment service provider servicing the account of the payment service user. The payers should give an explicit consent to the TPP to access their payment account and be properly informed about the extent of this access (Preamble, para. 51).

All provisions of PSD II have to be implemented in line with the rights and principles of the EU Charter of Fundamental Rights, including the right to respect for private and family life, the right to protection of personal data, the freedom to conduct a business, the right to an effective remedy and the right not to be tried or punished twice in criminal proceedings for the same offence (Preamble, para. 72). Moreover, any processing of personal data within the framework of PSD II has to be carried out in accordance with Directive 95/46/EC and Regulation (EC) No 45/2001 (Article 84).

Significantly, like the 2007 PSD, the proposed Directive does not apply to services provided by technical service providers, which merely support the provision of payment services, without entering at any time into possession of the funds to be transferred (Article 3(j)).

[20] Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC.

Regulation (EC) No 924/2009 on cross-border payments in the EU[21] and Regulation (EU) No 260/2012 on Technical and Business Requirements[22]

Regulation (EC) No 924/2009 on cross-border payments in the EU introduces several provisions that supplement the PSD and which are meant to further promote EU financial integration in general and SEPA implementation in particular. The Regulation's basic principle is that the charges for payment transactions offered by a payment service provider have to be the same for a payment of the same value, regardless of whether the payment is national or cross-border.

The Regulation applies to all electronically processed payments in the euro area, including credit transfers, direct debits, cash withdrawals at cash machines, payments by means of debit and credit cards, and money remittance. In addition, all non-euro area EU Member States have the possibility to extend the application of this Regulation and to apply the same charges for payments in euros as for payments in their national currency.

Providing technical details on the implementation of SEPA, Regulation No 260/2012 stipulates that the processing of personal data within the framework of Regulation No 924/2009 needs to comply with Directive 95/46/EC on the protection of personal data and on the free movement of such data. Moreover, Regulation No 260/2012 highlights that the introduction of SEPA and thus of common standards and rules for payments should take place in compliance with relevant national legislation on the protection of sensitive personal data and be geared towards safeguarding the interests of EU citizens (Preamble, para. 33).

4.1.2 Revised Tachograph Regulation[23]

In June 2012, the Council responded to European Commission plans for a merger of driving licences with tachograph driver cards and announced its intent to revise the 1985 Council Regulation (EEC) No 3821/85 on requirements for the construction, installation, use and testing of tachographs used in road transport (Article 1). The aim of the new draft legislation is to make tachograph fraud more difficult and to reduce administrative burdens by making use of new technologies and introducing a number of new regulatory measures.

Accounting for technological advances in the field, the proposal for a revised Regulation provides the legal framework for the use of three main technologies. First the proposed Regulation calls for a replacement of manual means of recording the location of vehicles by automated recording through satellite positioning. Second, the Regulation introduces

[21] Regulation (EC) No 924/2009 of the European Parliament and of the Council of 16 September 2009 on cross-border payments in the Community and repealing Regulation (EC) No 2560/2001 Text with EEA relevance.

[22] Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009 Text with EEA relevance.

[23] Proposal for a Regulation of the European Parliament and of the Council on tachographs in road transport and repealing Council Regulation (EEC) No 3821/85 and amending Regulation (EC) No 561/2006 of the European Parliament and the Council.

remote communication from the tachograph of basic information on compliance as a means to detect possible tachograph manipulation or misuse. Third, the Regulation suggests that tachographs may be equipped with an interface facilitating their integration into Intelligent Transport Systems (ITS).

In light of the technological changes proposed with regard the construction, installation, use and testing of tachographs, the proposed Regulation contains several provisions that are meant to ensure the protection of personal data. First, a vehicle's position will only be recorded between the point of departure at the beginning of the daily working period and the point of arrival at the end of the daily working period. Secondly, access to positioning data is only granted to competent control authorities. Thirdly, drivers have to give their explicit consent for access to personal data through an external ITS device.

4.1.3 Regulation for a Standardised and Secure System of Registries for the EU Emissions Trading Scheme (ETS)[24]

This Regulation sets out the principles and rules that govern the registries system, which accounts for transactions under the EU Emissions Trading Scheme (ETS). Registries are standardised and secured electronic databases containing common data elements to track the issue, holding, transfer and cancellation of emission units (Preamble, para. 1).

Under the Regulation, the European Commission is responsible for making available to national administrators data exchange and technical specifications necessary for exchanging data between registries and transaction logs, including the identification codes, automated checks, response codes and data logging requirements, as well as the testing procedures and security requirements necessary for the launching of data exchange (Article 105 (1)). The data exchange and technical specifications are drawn up in consultation with the Administrators' Working Group of the Climate Change Committee (Article 105 (2)).

The central administrator and Member States shall ensure that the Union Registry only stores and processes information concerning accounts, account holders and account representatives (Article 107 (1)). The central administrator and Member States also have to ensure that only personal data related to transactions that transfer Kyoto units are transferred (Article 107 (3)).

By way of derogation from these provisions, the central administrator or national administrator may provide data stored in the Union Registry to the following entities:

- The law enforcement and tax authorities of Member States
- The European Anti-fraud Office of the European Commission
- The European Court of Auditors
- Eurojust

[24] Commission Regulation (EU) No 389/2013 of 2 May 2013 establishing a Union Registry pursuant to Directive 2003/87/EC of the European Parliament and of the Council, Decisions No 280/2004/EC and No 406/2009/EC of the European Parliament and of the Council and repealing Commission Regulations (EU) No 920/2010 and No 1193/2011.

- The competent national supervisory authorities
- The national administrators of Member States (Article 110 (1)).

However, personal data may only be provided to these entities if their requests are justified and necessary for the purposes of investigation, detection, prosecution, tax administration or enforcement, auditing and financial supervision of fraud involving allowances or Kyoto units, or of money laundering, terrorism financing, other serious crime, or breaches of Union or national law ensuring the functioning of the ETS.

4.1.4 Fusion for Energy (F4E) Joint Undertaking

Composed of Euratom, which is represented by the European Commission, and the Member States of Euratom, Fusion for Energy (F4E) supports European industry and research organisations in developing and manufacturing technology components for ITER. ITER is the world's largest scientific partnership concerned with establishing fusion as a viable and sustainable source of energy. F4E also participates in the Broader Approach international agreement with Japan, which has been set up to promote cooperation on the development of fusion energy and to complement ITER by filling possible knowledge gaps.

Since its creation in 2008, F4E has provided its employees with full remote access to the ICT infrastructure, drawing on the Citrix application, which reproduces the environment of an onsite F4E workstation on a virtual desktop, which can be logged on to from any PC, laptop or tablet outside the F4E premises with a RSA key (Fusion for Energy 2008: 40). More recently, F4E has also begun to implement Regulation (EC) 45/2001 on the protection of personal data, providing F4E staff and external experts with the possibility of exercising their rights regarding the treatment of their personal data (Fusion for Energy 2012: 100). Moreover, F4E has implemented several measures to protect the F4E ICT environment against security incidents, also establishing a remote disaster recovery facility (Fusion for Energy 2009: 57).

4.2 Specific legal and political frameworks covering an Area of Freedom Security and Justice (AFSJ)

Most cybersecurity aspects of EU legal and policy frameworks in the domain of home affairs have been informed by pre-existing international legislation. Specifically, the 1981 Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the 2001 Additional Protocol to the 1981 Convention, and the 1987 CoE Recommendation R (87) 15 on Regulating the Use of Personal Data in the Police Sector have shaped EU home affairs legislation with regard to protecting the privacy of personal data and securing electronic information.

4.2.1 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (and the 2001 Council of Europe Additional Protocol to the Convention)

The 1981 CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data constitutes one of international law's principal instruments when it comes to governing the protection of individuals' right to privacy in the context of collecting, processing and transferring personal data electronically (Article 1). The data protection rules the Convention sets out are applicable to both the public and the private sector in countries that are parties to the Convention (Article 3(1)).

According to the Convention, electronically processed personal data must be obtained fairly and lawfully, used for specified and legitimate purposes in a form that permits identification of the data subjects for no longer than is absolutely necessary, and be adequate, relevant and not excessive in relation to the purposes for which it is used (Article 5). Data subjects are at all times expected to be able to gain information about the nature and purpose of personal data kept by a data controller as well as the identity and principal place of business of the data controller (Article 8).

With regard to ensuring the security of data collected and processed, the Convention rather superficially stipulates that appropriate security must be in place to protect personal data stored electronically against accidental or unauthorised destruction or accidental loss, as well as against unauthorised access, alteration or dissemination (Article 7).

Significantly, the Convention explicitly rules out the lawfulness of collecting and processing several specific categories of data unless appropriate safeguards are provided for by national law. These categories comprise personal data pertaining to:

- Racial origin
- Political opinions
- Religious or other beliefs
- Health or sexual life
- Criminal convictions (Article 6).

Derogations only apply when provided for in the national laws of parties to the Convention and when necessary for a 'democratic society' to protect national security, public safety, national monetary interests, the interests of data subjects, or the freedoms of others, or to pre-empt criminal offences (Article 9(2)). Derogations may also apply when personal data is used for statistical or scientific research purposes and no infringement of data subject's privacy occurs (Article 9(3)).

As regards the electronic transfer of personal data across the national boundaries of parties to the Convention, the CoE has not defined any legal caveats and instead refers to relevant national legislation (Article 12). However, in the 2001 Additional Protocol to the Convention, the CoE emphasises that parties to the Convention may only transfer personal data to entities in non-party countries when the data recipient is able to ensure adequate levels of protection for the data transfer (Article 2(1)) and there is no national law

providing for a derogation based on the specific interests of the data subject or legitimate public interests (Article 2(2)).

4.2.2 1987 Council of Europe Recommendation R (87) 15 on Regulating the Use of Personal Data in the Police Sector

Drawing on the 1981 CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Recommendation R (87) 15 elaborates a set of principles specifically related to the electronic collection, processing and transfer of personal data for law enforcement purposes (Appendix Principle 1).

According to the Recommendation, police forces of countries that are party to the 1981 Convention are only allowed to collect and process personal data that is accurate and indispensable for the performance of lawful police tasks (Principle 3) as well as the pre-emption of imminent danger or specific criminal offences (Principle 2). Significantly, the collection of data by means of technical surveillance or other electronic devices is not covered by the Protocol (Principle 2(3)). Data subjects are to be informed about the private data that is held in relation to them as soon as the object of the police activities is no longer likely to be prejudiced (Principle 2(2)).

To ensure the security of personal data, the Recommendation emphasises that the data holder must take all necessary measures to ensure the appropriate physical and logical security of the data and prevent unauthorised access, communication or alteration (Principle 8(1)). At the same time, the Recommendation stipulates that direct online access to personal data is subject to additional rules laid down in national law (Principle 5(6)).

Akin to the 1981 Convention, the Recommendation generally prohibits the collection of data on data subjects because they have a particular racial origin, religious conviction, sexual orientation or political opinion, or because they belong to particular movements or organisations that are not proscribed by law. However, in contrast to the 1981 Convention, the Recommendation declares the collection of such data permissible if absolutely necessary for conducting a particular enquiry (Principle 2 (4)).

The Recommendation stipulates that on the national level personal data can be transferred among all police bodies on the basis of a legitimate interest (Principle 5(1)). In contrast, other public bodies may only receive such personal data in one of four cases:

- A clear legal obligation or authorisation exists
- The data are vital to the performance of the recipient's lawful tasks and the transfer is also in line with the data holder's legal obligations
- The transfer is in the data subject's interest
- The transfer is vital to pre-empt a serious and imminent danger (Principle 5(2)).

On the basis of the Recommendation, international transfers of personal data may only be received by police bodies. They also require a relevant national or international legal basis unless the transfer is necessary to pre-empt a serious and imminent danger or a serious criminal offence that falls within the realm of ordinary law (Principle 5(3)).

In line with the Recommendation's general tone, the transfer of private data from police forces to private parties is only permissible when a clear legal obligation or authorisation exists (Article 5(3i)). However, the Recommendation also stipulates that the transfer of personal data to private parties can be permissible when such transfer is undoubtedly in the interest of the data subject and the data subject has either given his or her consent or the circumstances allow for a presumption of such consent, or if the transfer is necessary to pre-empt a serious and imminent danger (Article 5(3ii)).

4.2.3 Law Enforcement and Judicial Cooperation

European Police Office – Europol[25]

Europol's standards of data protection are largely modelled on the principles of Council of 1981 CoE Convention and the 1987 CoE Recommendation (Article 27). In addition, Europol is subject to several specific implementing rules and in particular the AWF Rules, which govern the handling of Europol's analysis work files.[26] Internally, Europol observes the principles of Regulation 45/2001 with regard to the processing of staff data.

Europol's databases are subject to the implementation of several information security measures. Europol has an obligation to implement the technological and organisational measures necessary to protect personal or other sensitive data (Article 35). Accordingly, several technological safeguards have been implemented at Europol to prevent unauthorised access to and use of data. In addition, protection measures against data loss or system malfunction have been put in place.

Each type of information requires a different set of security measures to be applied in order to protect it against unauthorised disclosure. Information classified CONFIDENTIAL or above may only be created or reproduced by duly authorised Confidentiality Officials using special secure equipment, in order to ensure full traceability (in the same way as hardcopies are concerned).

As far as data transfer within the EU is concerned, Europol has established and maintained cooperative relations with a list of EU institutions and agencies, such as Eurojust, the European Central Bank and the European Anti-Fraud Office (OLAF) (Article 22). Where no agreement has been concluded, Europol can still exchange information, including personal data, provided that the exchange is necessary for the pursuance of the data recipient's lawful tasks (Article 24).

In general, there are two types of cooperation agreement that Europol can enter into with third states or entities: strategic and operational agreements (Article 23). Strategic

[25] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol).

[26] The analysis work file (AWF) allows Europol analysts to work together with organised crime and terrorism specialists to gather criminal intelligence. AWFs cover all high-priority serious crime areas impacting the European Union. Analytical support can be provided remotely from Europol premises, or in the field. AWFs offer a variety of operational and strategic products that are shared among participants. Within an AWF, a specific target group or Joint Investigation Team can be set up to meet the needs of a group of Member States and to tackle a common criminal phenomenon.

agreements, which allow for the exchange of general intelligence, have been concluded with Albania, Bosnia-Herzegovina, Colombia, Moldova, Montenegro, Russia, Serbia, Turkey and Ukraine. Europol has also concluded an agreement with the UN Office on Drugs and Crime and the World Customs Organization.

However, personal data may only be transferred where an operational agreement is in place. Europol may conclude such an agreement with third parties that have an adequate level of data protection. The process for concluding an operational cooperation agreement involves a prior data protection assessment of the third party to ensure that the necessary data protection and confidentiality rules are in place and in practice. As of 2013, the states with which an operational agreement has been concluded are Australia, Canada, Croatia, the Republic of Macedonia, Iceland, Monaco, Norway, Switzerland and the USA. In addition, Europol has an operational cooperation agreement with Interpol and Eurojust.

In the absence of a cooperation agreement, personal data can be transferred to third states to pre-empt an imminent threat. Europol may thus transmit personal data where it is absolutely necessary to safeguard the essential interests of EU Member States concerned within the scope of Europol's objectives or in the interests of preventing imminent danger associated with crime or terrorist offences (Article 23 (8)).

Europol Information System (EIS)[27]

The range of data that may be processed in the EIS is limited in several important ways. Only data that are necessary for the performance of Europol's tasks, including name, date and place of birth, nationality, sex, place of residence, profession, identification documents, fingerprints and DNA profiles (Article 12 (2)) may be used (Article 12 (1)). Data in the EIS must relate to suspects, convicted criminals or persons for whom there are factual indications or reasonable grounds to believe that they will commit crimes that fall within Europol's mandate.

Europol may only store data in the EIS for well-defined periods of time (Article 20). In general, information shall only be held for as long as is necessary. In line with this, data must be deleted from the EIS when persons have been acquitted or proceedings against them have been definitively dropped (Article 12(5)).

Secure Information Exchange Network Application (SIENA)[28]

Akin to the regulations governing the EIS, Europol must implement several data protection principles and information security safeguards with regard to operating SIENA. Europol is obliged to keep a record of transmissions. Taking this into account, the SIENA system automatically documents all communication processes. To further ensure the responsible handling of personal data, information is only transmitted by Europol to other

[27] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol).
[28] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol).

partners if the recipient gives an undertaking that the data will be used only for the purpose for which they were transmitted (Article 24 (2)).

Eurojust[29]

In order to reinforce the fight against serious organised crime, the 1999 Tampere European Council decided on the setting up Eurojust, which is a network composed of prosecutors, magistrates or police officers of equivalent competence (Preamble, para. 3).

In order to achieve its objectives, Eurojust processes personal data by automated means or in structured manual files. In this respect, Eurojust is expected to guarantee a level of data protection that corresponds at least to that which results from the application of the principles of the 1981 CoE Convention and the 2001 Additional Protocol to the Convention (Preamble, para. 9).

Prüm Convention[30]

The Prüm Decision provides for the automated exchange of DNA, fingerprints and vehicle registration data, as well as for other forms of police cooperation between the 28 EU Member States. Access to DNA profiles and fingerprints held in national databases is granted on a 'hit/no-hit' basis, which means that DNA profiles or fingerprints found at a crime scene in one EU Member State can be compared with profiles held in the databases of other EU Member States. Car registration data (including licence plates and chassis numbers) are exchanged through national platforms that are linked to the online application 'EUCARIS'.

Financial Intelligence Unit Cooperation[31]

According to the Council decision on the cooperation of EU Member State Financial Intelligence Units (FIU), Member States shall ensure that FIUs, set up or designated to receive disclosures of financial information for the purpose of combating money laundering, cooperate to assemble, analyse and investigate relevant information on any fact that might be an indication of money laundering (Article 1(1)). To this end, EU Member States shall ensure that national FIUs exchange any available information that may be relevant to the processing or analysis of information or to investigation by the FIU regarding financial transactions related to money laundering and the natural or legal persons involved (Article 1(2)).

---

[29] Council Decision of 28 February 2002 on setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA).

[30] Convention of 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration.

[31] Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA).

The information transferred in this context, including the transfer of personal data, is protected, in conformity with the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data and taking account of Recommendation No R(87)15 of 15 September 1987 of the Council of Europe Regulating the Use of Personal Data in the Police Sector, by at least the same rules of confidentiality and protection of personal data as those that apply under the national legislation applicable to the requesting FIU (Article 5(5)).

Exchange of Information on International Football Hooliganism[32]

With the aim of preventing and combating football-related violence, this Decision defines a framework for the exchange of relevant information among competent police authorities in EU Member States (Preamble, para. 4). In this respect, the Decision also formulates several guidelines for the establishment of a national police football information point in each Member State (Preamble, para. 5).

The Decision stipulates that the collection, processing and transfer of personal data among law enforcement agencies has to comply with the rules set out in the 1981 CoE Convention and shall be protected in accordance with the Convention and the 2001 Additional Protocol to the Convention. In addition, the principles of the 1987 CoE Recommendations are to be taken into account when law enforcement authorities handle personal data obtained under the Decision (Article 8(1)). More generally, the transfer of personal data is limited to what is necessary for implementing appropriate measures to maintain law and order when a football event takes place. Such exchange may in particular involve details of individuals actually or potentially posing a threat to law and order and security (Article 3(3)).

European Arrest Warrant (EAW)[33]

The 2002 Framework Decision on the European Arrest Warrant (EAW) requires each EU Member State's national judicial authorities to serve requests for the extradition of a person made by the judicial authority of another EU member state. The transmission of an extradition request can be effected via the secure telecommunications system of the European Judicial Network (Article 10(2)).

The personal data processed in the context of the implementation of the European Arrest Warrant Framework Decision are to be protected in accordance with the principles of the 1981 CoE Convention (Preamble, para. 14).

[32] Council Decision of 25 April 2002 concerning security in connection with football matches with an international dimension (2002/348/JHA).

[33] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

Simplifying the Exchange of Information between Law Enforcement Authorities[34]

The Council Framework Decision on Simplifying the Exchange of Information between Law Enforcement Authorities establishes a set of rules under which EU Member State law enforcement authorities may exchange existing information and intelligence for the purpose of conducting criminal investigations or criminal intelligence operations (Article 1(1)). Adopted in the wake of the Madrid terrorist attacks, the Framework Decision first and foremost aims to improve cross-country information exchange, for example by fixing a time frame for responding to requests.

The Framework Decision stipulates that the collection, processing and transfer of personal data among law enforcement agencies has to comply with rules set out in the 1981 CoE Convention and shall be protected in accordance with the Convention and the 2001 Additional Protocol to the Convention. In addition, the principles of the 1987 CoE Recommendations are to be taken into account when law enforcement authorities handle personal data obtained under the Framework Decision (Article 8(1)). At the same time, all information and intelligence processed under the Framework Decision is subject to the data protection provisions applicable in the country that hosts the data recipient.

Asset Recovery Offices Cooperation[35]

This Council Decision governs the cooperation of EU Member State authorities involved in the tracing of illicit proceeds and other property that may become liable to confiscation (Preamble, para. 3). Specifically, the Decision defines procedures related to the rapid exchange of information among national Asset Recovery Offices (Preamble, para. 4).

Echoing the Council Framework Decision on Simplifying the Exchange of Information between Law Enforcement Authorities, the Decision stipulates that the collection, processing and transfer of personal data among national Asset Recovery Offices has to comply with the relevant rules set out in the 1981 CoE Convention and shall be protected in accordance with the Convention and the 2001 Additional Protocol to the Convention. In addition, the principles of the 1987 CoE Recommendations are to be taken into account when the authorities handle personal data obtained under the Decision (Article 5(2)). At the same time, all information and intelligence processed under the Decision is subject to the data protection provisions applicable in the country that hosts the data recipient.

---

[34] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

[35] Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime.

Mutual Recognition of Judgements and Probation[36]

The Framework Decision on the Mutual Recognition of Judgements and Probation aims to facilitate the social rehabilitation of sentenced persons, improving the protection of victims and of the general public, and facilitating the application of suitable probation measures and alternative sanctions, in case of offenders who do not live in the country of conviction. With a view to achieving these objectives, the Framework Decision lays down a number of rules, according to which EU Member States have to recognise judgments and probation decisions made and to supervise probation measures imposed in other Member States with regard to persons residing on their territory (Article 1 (1)).

Personal data processed in the context of implementing the Framework Decision has to be protected in line with the rules defined in the 1981 CoE Convention (Preamble, para. 23).

4.2.4 Common European Asylum System

EURODAC Regulation[37]

The EURODAC Regulation provides a legal framework for the creation and maintenance of the EURODAC infrastructure, which enables the collection and analysis of fingerprint data of third-country nationals and stateless persons who are making claims to an EU Member State for international protection (Article 1).

Addressing several data protection aspects, the Regulation stipulates that fingerprint data processed through EURODAC may be accessed by Member States' relevant institutions and by Europol for criminal intelligence purposes when assessing an applicant's claim for international protection (Article 2).

The Regulation highlights that the integrity of fingerprint data is maintained through a dedicated encrypted communication infrastructure between EURODAC's 'Central System' and Member States, with each Member State having a single National Access Point that is subject to the transmission guidelines of the Central System (Article 2). Following a transmission of an applicant's data from a Member State to the Central System, the latter records a variety of data besides just the fingerprint signature, including personal data on the applicant and a record of their application for international protection (Article 11)

---

[36] Council Framework Decision 2008/947/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions.

[37] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of EURODAC for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast).

With regard to data integrity and security, the Regulation stresses that Member States are responsible for the security of the data that they send to and receive from the EURODAC Central System (Article 23), while the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice is responsible for establishing the technical requirements necessary for secure electronic transmission (Article 24).

4.2.5 Schengen, Borders and Visas

Second-generation Schengen Information System (SIS II) Decision[38]

The second-generation Schengen Information System (SIS II) will replace the current system, providing enhanced functionalities (see Section 2.5.4). It is currently undergoing extensive testing in close cooperation with EU countries and associated countries participating in the Schengen area.

The SIS II Decision includes provisions on the technical aspects and operation of SIS II, responsibilities of the management authority and of participating countries, processing of data relating to alerts that will be contained in the system, and conditions for data access and protection. With regard to the later, the Decision invokes the 1981 CoE Convention according to which personal data in relevant SIS II alerts concerning police and judicial cooperation in criminal matters must be protected, and as the basis for defining categories of data whose processing in SIS II will be prohibited (Preamble, para. 19).

Visa Information System (VIS) Regulation[39]

The Visa Information System (VIS) Regulation defines the purpose and functionalities of, as well as the responsibilities for, the VIS. It provides the conditions and procedures for the exchange of visa data between EU countries and associated countries applying the common visa policy. The examination of applications for short-stay visas and decisions on extending, revoking and annulling visas, as well as checks on visas and the verifications and identifications of visa applicants and holders are facilitated.

With regard to data protection, the Regulation stresses the responsibility of Member States to provide data subjects with information on the identity and contact details of the data controller, the purposes for which the data is processed within the VIS, the categories of the recipients of the data, the period of retention of the data and the right to access, correct and delete the data (Article 38). Moreover, each EU Member State must task a National Supervisory Authority, established in accordance with Directive 95/46/EC, to monitor the lawfulness of the processing of personal data by that country (Article 37 (2)).

---

[38] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

[39] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

Naples II Convention[40]

The Naples II Convention sets out a framework for cooperation and mutual assistance among EU Member State customs administrations with a view to:

- Preventing and detecting infringements of national customs provisions
- Prosecuting and punishing infringements of Community and national customs provisions (Article 1).

The electronic exchange of personal data among EU Member State customs administrations under the Naples II Convention is supposed to respect the 1981 CoE Convention (Article 25 (1)).

4.3 Specific frameworks covering CSDP and CFSP

4.3.1 Protection of EU classified information for CSDP

An increasingly varied set of rules, policies and guidelines govern the protection of classified information in the EU in the context of Common Security and Defence Policy. These apply to relevant EU-level institutions (EEAS, GSC, OHQ Cell at SHAPE) and relevant Member States (Operational HQs designated as such by Framework Nations[41]) as well as those participating Member States contributing troops (known as Troop Contributing Nations) to CSDP operations. These have been released in 2011.[42] Primarily, classified information is transmitted in Computer Information Systems (CIS) used by the EEAS and Member States for intelligence, military and security purposes relating to CSDP. They follow a fairly standard definition of Information Assurance and take the form of Information Assurance Security Policies (IASPs – which are obligatory) and Information Assurance Security Guidelines (IASGs – which are voluntary). This model of high-level frameworks set as obligatory instruments and more detailed context-dependent guidance follows that of the rules governing information security more generally described in Chapter 2.

Risk Management is specified in a policy document issued by the General Secretariat of the Council in 2003 and applies to all EU classified information.

Agreements have also been concluded between the EU and Member States (2011) and also between the EU and foreign countries and international organisations including NATO[43], the UN[44] and the ICC.[45]

---

[40] Council Act 98/C 24/01 of 18 December 1997 drawing up, on the basis of Article K3 of the Treaty on European Union, the Convention on mutual assistance and cooperation between customs administrations.

[41] France, Germany, Greece, Italy and the UK

[42] 03/05/2011(CSG 10872/11) and 23/03/2011(CSG 8054/11).

[43] GSC 10006/03.

[44] GSC 16008/04.

4.3.2 EU Council Security Rules

An EU-level network defence policy is defined in IASP 4 (ST-8408/12).[46] The Information Assurance Security Guidelines on Network Defence IASG 4-01 were agreed by the European Council security committee in 2012 in accordance with the Council Security Rules (CSD) and are aimed at supporting the implementation of these rules and IASP 4.

These guidelines define minimum standards to be observed for the purposes of network defence of CIS and interconnections between them. The need for network defence is seen as increasingly important given a varied, persistent, powerful and more acute threat landscape, and the varied and complex nature of interdependent CIS. The guidelines apply to EU institutions (as defined under Title V, Chapter 2 of the TEU) and Europol and Eurojust as a reference for implementing security rules in their own structures. Furthermore Member States must use the security guidelines as a benchmark when handling EU classified information in national structures (such as might be required when a Framework Nation is provided an Operational HQ for the operational control of a EU-led CSDP Operation). The guidelines are grouped into three areas: Security Assurance (Chapter III); Security Operation and Maintenance (Chapter IV); and Security Restoration (Chapter V) and Management Commitment (Chapter VI).

Security assurance deals with design and development; the provision of technical protection; and awareness training of users. Security operation and maintenance addresses configuration and change management; alert management and patch management; ongoing event logging, monitoring and consolidation; network discovery, mapping and monitoring; generation of security alerts and warnings; implementation considerations; and rule set review. Security restoration includes topics on incident investigation and digital forensics; incident response and corrective action; business continuity and disaster recovery planning; and information sharing and escalation mechanisms. Finally, management review encompasses measures to review progress of improvement of CIS; confirm that network defence measures are consistent with the evolving threat scenario; and other inputs (e.g. incidents) that might suggest that the network defence measures need adjustment.

4.4 Conclusion

This chapter has discussed a broad range of EU activities that are somewhat unique due to their scale (involving information exchange amongst administrations in 28 different countries). We have seen that application areas sometimes require very specific security or privacy governance arrangements. These arrangements are sometimes at odds with the potential benefits that more advanced models of technology service and delivery can offer

[45] Official Journal of the European Union, *Agreement between the International Criminal Court and the European Union on cooperation and assistance,* 28 April 2006

[46] Council Communication 10578/12 of 6 June 2012 on Information Assurance Security Guidelines on Network Defence

(such as, for example, cloud computing). Indeed, it is perhaps less realistic to consider the deployment of new technologies, such as cloud computing, in areas that are seen as more exotic, such as, for example, the storage and access of forensic data in the Europol Information System.

Furthermore, the use of more sophisticated technology for CSDP operations is at a very early stage of maturity and will be primarily driven by Member States' progress in developing capability in these domains. An issue closely related to this is the extent to which a model of Network Enabled Capability (NEC) takes hold in the CSDP realm, which would require more sophisticated security frameworks. Another consideration is the extent to which open architectures and big data could be leveraged for EU-led crisis management operations (e.g. through open geospatial data or crowd-sourced social media intelligence). Such a development would require that security and privacy frameworks significantly evolve from the current situation described in this chapter.

Nonetheless there are some interesting developments within EU institutions and agencies with regard to technology adoption. These include, for example, the noted use of cloud computing services by the ESA in the context of the Copernicus Programme for geospatial monitoring. The recognition encompassed in the Council Network Defence Guidelines that the multi-disciplinary heterogeneous nature of some types of EU activity requires evolutionary thinking in approaching information risk management is another good example.

5. Conclusions

This study reveals the complex landscape that underpins the use of ICT by EU institutions and agencies.

We have seen that there is a wide range of business rationales among EU institutions and agencies, which place different requirements upon information technology. These rationales resonate with those that can be encountered in other large public sector administration (procurement, human resources, document management, and processing). However, there are also other requirements that are unique to the external-facing mandates of EU institutions and agencies: for example, supporting coordination between EU Member States with regard to the internal market, contributing to an area of freedom, security and justice, supporting law enforcement and criminal justice cooperation, or the processing of information for military and crisis management operations as well as the conduct of foreign and security policy.

A review of the relevant legal and policy frameworks demonstrates that there are a number of common instruments that aim to address information security and data protection issues in light of the diversity of rationales for the use of technology. These instruments constitute obligatory and voluntary guidelines, covering information security in general, data protection, EU classified information, and access to public information and documents.

There are also a number of specific security and privacy frameworks covering unique thematic areas. These include law enforcement and judicial cooperation, borders, visas, and the Schengen area of free movement, as well as EU-led crisis management operations. These policy domains require specific legal and policy frameworks covering information security and data protection, not least because they deal with either sensitive information relating to intelligence on suspects or classified information whose compromise might have varying degrees of impact to an EU-led crisis management operation.

The challenges related to introducing new technologies in EU institutions and agencies, such as BYOD or cloud computing, for example, are still only partly revealed. In relation to the horizontal frameworks, it is clear that there is a balance to be struck: some of the new models of technology service delivery, especially cloud computing and service-orientated architectures, hold promises of efficiency but the prevailing EU legal and policy frameworks may inhibit their take up. With security and privacy frameworks covering specific thematic areas covered in the penultimate chapter, it may be that, at this stage, the

unique characteristics of these domains are likely to inhibit any more extensive usage of cloud computing or many other new technologies for that matter.

Bibliography

Council of the European Union (2009), *Single Progress Report on the Development of the EU Military Capabilities, 8715/09*. Brussels: Mimeo.

ENISA (n.d.), *Inventory of Risk Management/Risk Assessment Tools*. As of 14 February 2014: http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-tools

European Commission (2010), *Communication SEC(2010) 1182 final to the Commission on getting the best from IT in the Commission*. Brussels: Mimeo.

European Commission (2011), *Communication SEC(2011) 1500 final to the Commission on first decisions in the IT rationalisation process*. Brussels: Mimeo.

European Commission (2012a*), e-Commission 2012–2015 Communication SEC(2012) 492 to the Commission from Commission Vice President Šefčovič on delivering user-centric digital services*. Brussels: Mimeo.

European Commission (2012b), *Communication COM(2012) 179 final from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a strategy for e-procurement*. Brussels: Mimeo.

European Commission (2012c), *Communication COM(2012) 529 final from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on unleashing the potential of cloud computing in Europe*. Brussels: Mimeo.

European External Action Service (2012), *Impetus: Bulletin of the EU Military Staff. Autumn/Winter 2012*. As of 14 February 2014: http://eeas.europa.eu/csdp/documents/pdf/final_impetus_04_oct_12_en.pdf

European Union Satellite Centre (2012), *Annual Report 2012*. Madrid: European Union Satellite Centre. As of 14 February 2014: http://www.satcen.europa.eu/images/stories//eu%20satcen%20annual%20report%202012.pdf

Fusion for Energy (2008), *Annual Report 2008*. Barcelona: The European Joint Undertaking for ITER and the Development of Fusion Energy. As of 14 February 2014: http://fusionforenergy.europa.eu/downloads/mediacorner/publications/reports/F4E_Annual_Report2008.pdf

Fusion for Energy (2009), *Annual Report 2009*. Barcelona: The European Joint Undertaking for ITER and the Development of Fusion Energy. As of 14 February 2014: http://fusionforenergy.europa.eu/downloads/mediacorner/publications/reports/ANNUAL_2009.pdf

Fusion for Energy (2012), *Annual Report 2012*. Barcelona: The European Joint Undertaking for ITER and the Development of Fusion Energy. As of 14 February 2014: http://fusionforenergy.europa.eu/downloads/mediacorner/publications/reports/ANNUAL_2012.pdf

Moran, F. (2010), *Presentation on 'Trust and Security in the e-Commission', delivered at the Trust in the Information Society Conference, 10–11 February 2010, Leon, Spain*. As of 14 February 2014: http://trustworthyict.inteco.es/docs/S2-06-Trust_and_Security_in_the_e-Commission-Francisco_Moran.pdf

Rehrl, J., & Weisserth, H.-B. (2012), *Handbook on CSDP, 2nd Edition*. Vienna: Federal Ministry of Defence and Sports of the Republic of Austria.

Robinson, N., et al. (2013), *Data and Security Breaches and Cyber-Security Strategies in the EU and Its International Counterparts*. Brussels: European Parliament.

Tamai, S. (2009), 'Tools for Operational Planning Functional Area Service: what is this?', *NRDC-ITA Magazine, Issue 14*. As of 14 February 2014: http://www.nato.int/nrdc-it/magazine/2009/0914/0914h.pdf

Wellens, P. (2013), *Presentation on 'Testa new generation', delivered at the 2nd International Conference on Cyber Crisis Cooperation and Exercises, 23–24 September 2013, Athens, Greece*. As of 14 February 2014: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/presentations/pieter-wellens-digit-the-stesta-infrastructure.pdf